Switch CLI Configuration Manual

Corresponding Software Version：Release 5.0.x

Document Version ： V1.07

Release Time：2020.12.25

1.System Management

1.1. CLI Mode

The device CLI management interface is divided into several different modes. The command mode the user is currently in determines the commands that can be used. Enter the question mark key (?) at the command prompt to list the supported commands for each command mode. When a user logs into a device, it is first in user mode.

Mode Name	Prompt	switch mode	Description
User Mode	SWITCH>	Configure "enable" to switch to privileged mode	Support device information display, debugging command line, etc.
Privileged mode	SWITCH#	Configure terminal to switch to global mode; configure dial to switch to user mode	Support network testing; Support function module information viewing; Support configuration save, clear and other operations
Global Mode	SWITCH(config)#	Configure exit to switch to privileged mode; configure interface to switch to interface mode	Support for global-based configuration commands
interface mode	SWITCH(config-if)#	Configure exit to switch to global mode; configure end to switch to privileged mode	Support configuration commands in interface mode, interfaces include physical interfaces, aggregated interfaces, and SVI interfaces

1.2. CONFIGURE MANAGEMENT IP

1.2.1. Configuration Commands

●Configure the device IPv4 management IP

Command	SWITCH(config)#**management vlan** VLANID **ip address** IPADDR/MASKLEN **gateway** IPADDR SWITCH(config)#**no management vlan**
Description	Configure/Delete Device IPv4 Management IP

●Configure the device Ipv4 management IP DHCP dynamic acquisition

Command	SWITCH(config)#**management vlan** VLANID **ip address dhcp** SWITCH(config)#**no management vlan**
Description	Configure/Delete Device IPv4 Management IP

●Configure the device IPv6 management IP

Command	SWITCH(config)#**management vlan** VLANID **ipv6 address** IPV6ADDR/MASKLEN **gateway** IPV6ADDR SWITCH(config)#**no management vlan**
Description	Configure/Delete Device IPv6 Management IP

●Configure the device Ipv6 management IP DHCP dynamic acquisition

Command	SWITCH(config)#**management vlan** VLANID **ipv6 address dhcp** SWITCH(config)#**no management vlan**
Description	Configure/Delete Device IPv6 Management IP

●View device management IP configuration

Command	SWITCH#**show management summary**
Description	Configure/Delete Device IPv6 Management IP

1.2.1. **Configure Case**

Case Requirement: Manage VLAN is 1，Maneged IP is 192.168.64.200/24，The gateway address is 192.168.64.1

Enter Global Mode:

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Configure Ipv4 Manage IP:

```
SWITCH(config)#management vlan 1 ip address 192.168.64.200/24 gateway
192.168.64.1
```

View management IP configuration information:

```
SWITCH#show management summary
Management interface with Ipv4:
Type:        Static
Vlan:        1
Ip address:  192.168.64.200/24
Gateway:     192.168.64.1
```

1.3. CONFIGURATION SAVE/CLEAR OPERATION

- Configure save command

Command	SWITCH#write
Description	Save Configuration

●Restore default configuration command

Command	SWITCH#**copy default-config startup-config** SWITCH#**reload**
Description	Restore the system default configuration, which will take effect after the device restarts

1.4. DVICE HOT RESTART OPERATION

- Configure HOT RESTART Command

Command	SWITCH#**reload**
Description	Device Hot Restart

1.5. USER LOGIN MANAGEMENT

- Add/delete users, modify user passwords

Command	SWITCH(config)# **username** NAME **password** LINE SWITCH(config)# **no username** NAME
Description	If the user NAME does not exist, add a new user, if it exists, modify the user's password; By default, the device comes with user "admin" and password "admin", which supports password modification and deletion operations; The device supports up to 8 users, and the length of the user and password is 0-32 bytes; The password display is encrypted; Password characters are case sensitive; The delete operation does not support deleting the user itself; to delete an online user, the user must be kicked off the line first;

- Forcing Online Users offline

Command	SWITCH# **clear line** {**vty | console**} LINE

Description	VtyIndicates a remote login user Console indicates the serial port login user; LINE information can be viewed in the show users command; Does not support forcing the user itself;

- Configuration to enable WEB management

Command	SWITCH(config)# **web-server enable** {**all | http | https**} SWITCH(config)# **no web-server enable**
Description	Configure Enable WEB management Default enable state Support Ipv6

- Configure enable Telnet Management

Command	SWITCH(config)# **telnet-server enable** SWITCH(config)# **no telnet-server enable**
Description	Configure enable telnet management Default disable state Support Ipv6

- Configure enable SSH management

Command	SWITCH(config)# **ssh-server enable** SWITCH(config)# **no ssh-server enable**
Description	Configure enable SSH management Default disable state Support Ipv6

Display command:

```
OLT#show users
Type      Line    User                Host(s)     Idle         PID
con         0       admin               idle        00:00:03     1932
```

1.6. CONFIGURE SYSTEM NAME

- Configure system name

Command	SWITCH(config)# **hostname** WORD
Description	Set the system name, the name must be composed of printable characters and the length cannot exceed 63 bytes; The configuration takes effect immediately

1.7. CONFIGURE SYSTEM UPGRADE

- Configure system upgrade

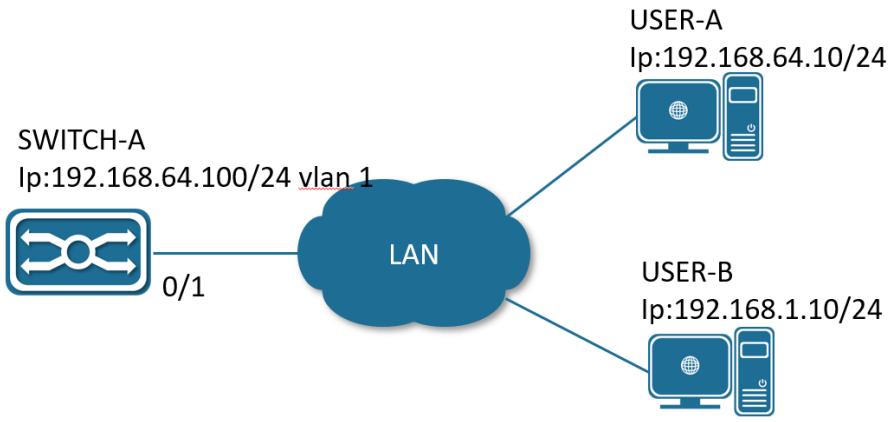
Command	SWITCH# **upgrade tftp tftp://**SERVER/FILENAME
Description	For firmware upgrade commands, you need to build a TFTP server on the terminal and ensure that the terminal and the device network are interconnected in both directions. SERVER: The IP of the TFTP server and the relative address of the server window and the firmware upgrade file. FILENAME: Firmware upgrade file. The firmware upgrade process will take 5-6 minutes, reboot the device to complete the firmware upgrade. Do not power off the device during the upgrade process.

Configuration case:

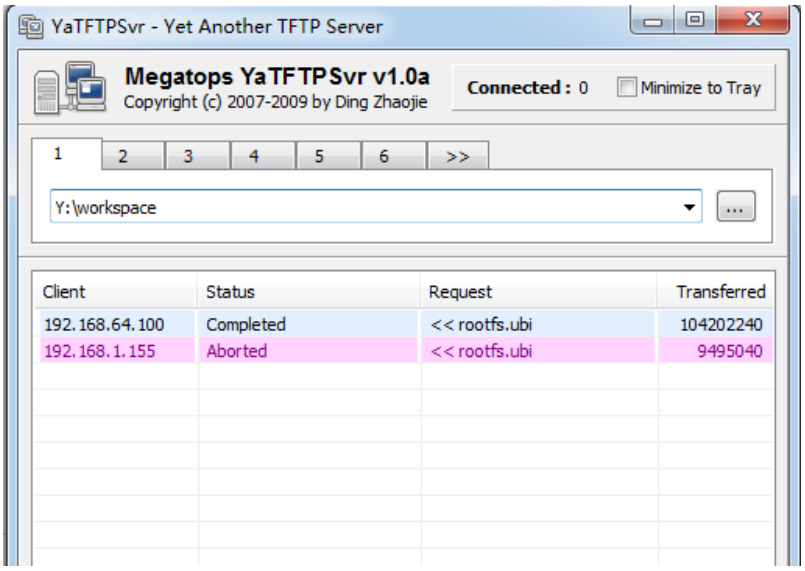
Case Requirement: Remote telnet to complete the firmware upgrade operation

1 see the following photogram, SWITCH-A is the equipment to be upgraded, turn on the telnet function;

USER-A is the host on the same network segment in the local area network, and USER-B is the management device in the local area network, both of which can log in to SWITCH-A by teleent.



2 Select USER-B to perform the version upgrade operation. Open the TFTP server on USER-B and place the upgrade file xcat-release-3.2.0.bin in the Y:/workspace directory.



3 USER-B telnet logs in to SWITCH-A, and executes the upgrade command in privileged mode.

```
SWITCH#upgrade tftp tftp://192.168.1.10/xcat-release-3.2.0.bin
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 55.5M    0 55.5M    0     0  1016k      0 --:--:--  0:00:55 --:--:-- 1033k
100 55.5M    0 55.5M    0     0  1016k      0 --:--:--  0:00:55 --:--:-- 1016k
Un-packet install file, this will last about 60 seconds.
Check upgrade file success.
Start erase and write bin to flash, this will last about 120 seconds.
Erasing 128 Kibyte @ 680000 --  2 % complete flash_erase: Skipping bad block at 006a0000
Erasing 128 Kibyte @ 12a0000 --  7 % complete flash_erase: Skipping bad block at 012c0000
Erasing 128 Kibyte @ 3580000 -- 21 % complete flash_erase: Skipping bad block at 035a0000
Erasing 128 Kibyte @ f5e0000 -- 100 % complete
Bad block at 6a0000, 1 block(s) from 6a0000 will be skipped
Bad block at 12c0000, 1 block(s) from 12c0000 will be skipped
Bad block at 35a0000, 1 block(s) from 35a0000 will be skipped
Reboot system to finish upgrade? (y/n):
```

4 After the upgrade command is executed, select "y" to restart the device to complete the upgrade, and select "n" to continue running the device. The upgrade operation will be completed after the next device restart.

1.8. CONFIGURE SYSTEM TIME

- Manually configure the system time

Command	SWITCH# **clock set** HH:MM:SS DAY MON YEAR
Description	Set system time such as Clock set 15:30:00 1 october 2017

- Configure ntp Server

Command	SWITCH(config)# **ntp server** A.B.C.D
Description	Configure the IP address of the NTP server (domain name configuration is not supported). After the configuration is complete, if the device and the server are connected to the network, the device will automatically synchronize the time information from the server. It takes about 4-8 minutes to complete the time synchronization for the first time.

- CONFIGURE SYSTEM TIME ZONE

Command	SWITCH(config)# **clock timezone** ZONE
Description	Configure the system time zone, the default is UTC, which supports standard time zone configuration, such as Shanghai time zone keyword "Shanghai", Hong Kong time zone keyword "Hong_Kong", etc.

- View system time

Command	SWITCH# **show clock**
Description	View the system time

2. CONFIGURE INTERFACE

2.1. DESCRIPTION OF THE INTERFACE TYPE

The interfaces of switching equipment can be divided into the following two categories according to the service level: Layer 2 interfaces and Layer 3 interfaces.

Layer 2 interface (L2 interface), including common physical port (Switch Port) and aggregation port (Port Channel).

Switch Port consists of a single physical port on the device, and only has the function of Layer 2 switching. The port can be an Access Port, Hybrid Port or a Trunk Port. You can configure a port as an Access Port, Hybrid Port or Trunk Port through the Switch Port interface configuration command.

Port Channel is referred to as PO, which is formed by the aggregation of multiple physical member ports. We can bundle multiple physical links together to form a simple logical link, which we call an aggregate port. For Layer 2 switching, the aggregation port is like a high-bandwidth Switch port, which can superimpose the bandwidth of multiple ports to expand the link bandwidth.

Layer 3 interface (L3 interface), here mainly refers to the SVI (Switch virtual interface) port.

SVI is a switching virtual interface, which is used to implement the logical 9 interface of Layer 3 switching. SVI can be used as the local management interface, through which the administrator can manage the device. You can create an SVI with the interface vlan interface configuration command, and then assign an IP address to the SVI to establish routing between VLANs.

2.2. CONFIGURE COMMAND

- Configure interface range

Command	SWITCH(config)# **interface** IFNAME_RANGE
Description	IFNAME_RANGE format such as gigabitEthernet 0/1-4, gigabitEthernet 0/9-12; When there are multiple range combinations, separate them with ',' without spaces; Support up to 5 range combinations; When the configuration of a port in the middle fails, the configuration is returned, and the subsequent port configuration is not continued.

- Configure the port descriptor

Command	SWITCH(config-if)# **description** DESC

Description	Configuration interface descriptor, up to 80 characters

- Configure port enable

Command	SWITCH(config-if)# **shutdown** SWITCH(config-if)# **no shutdown**
Description	Close the port or enable the port, it is enabled by default; Only supports configuration on physical ports

- Configure the port rate

Command	SWITCH(config-if)# **speed** {**10 | 100 | 1000 | auto**} SWITCH(config-if)# **no speed**
Description	Configure the port rate. When it is configured as auto or no speed, the port rate enters auto-negotiation mode; Default port rate auto-negotiation; Configuration on aggregate member ports is not supported; Configuration on SVI port is not supported

- Configure Port duplex

Command	SWITCH(config-if)# **duplex** {**auto | full | half**} SWITCH(config-if)# **no duplex**
Description	Configure port duplex. When configured as auto or no duplex, port duplex enters auto-negotiation mode; Default port duplex auto-negotiation; Configuration on aggregate member ports is not supported; Configuration on SVI port is not supported

Illustration

✦When both rate and duplex exit auto-negotiation mode, port auto-negotiation is closed

- Configure port flow control

When both the local switch and the peer switch have the flow control function enabled, if the local switch is congested:

The local switch will send a message to the peer switch to notify the peer switch to temporarily stop sending packets or slow down the speed of sending packets.

After receiving the message, the peer switch will suspend sending packets to the local end or slow down the speed of sending packets, thereby avoiding the occurrence of packet loss and ensuring the normal operation of network services.

Command	SWITCH(config-if)# **flowcontrol** {**on	off	auto**}
Description	Configure port flow control, default port flow control auto-negotiation; Configuration on aggregate member ports is not supported; Configuration on SVI port is not supported

- Configure Port MTU

When a port is exchanging high-throughput data, it may encounter a frame larger than the Ethernet standard frame length, which is called a jumbo frame. The user can control the maximum frame length that the port is allowed to send and receive by setting the MTU of the port. MTU refers to the length of the valid data segment in a frame, excluding the overhead of Ethernet encapsulation. Frames received or forwarded by the port, if the length exceeds the set MTU, will be discarded.

Due to chip restrictions, the MTU value only supports even numbers. If the user configures an odd number, the device will automatically align. For example, if the MTU is configured as 127, it actually supports 128-length packets to pass through.

Command	SWITCH(config-if)# **mtu** LENGTH SWITCH(config-if)# **no mtu**
Description	Configure the port MTU, the allowed range is 64~10240 bytes, the default is 1526 bytes Configuration on aggregate member ports is not supported; Configuration on SVI port is not supported

- Configure SFP Port Mode

By default, SFP ports are in 1000BASE-X mode and can support 1000BASE-X compliant SFP modules. Some optical modules (some 1000BASE-T SFP modules and some 100BASE-FX SFP modules) use the SGMII protocol, which can be supported by switching the port to SGMII mode. The port bandwidth can be increased to 2.5G by configuring the port mode 2500BASE-X, but only the specific models of SFP modules provided by our company are supported.

Command	SWITCH(config-if)# **port mode** {**sgmii	2500BASE-X	1000BASE-X}** SWITCH(config-if)# **no port mode**

Description	Default in 1000BASE-X mode; Sgmii: Configure the SFP port mode to SGMII mode; 2500BASE-X: Configure port 2500BASE-X mode, support 2.5G bandwidth; Only supports configuration on physical ports

- Configure port Isolation

In some application environments, it is required that some ports of the device cannot communicate with each other, which can be achieved by setting these ports as isolated ports. When the port is set as an isolated port, the isolated ports cannot communicate with each other, the isolated port and the non-isolated port can communicate normally, and the non-isolated port and the non-isolated port can communicate normally.

Command	SWITCH(config-if)#**switchport isolate** SWITCH(config-if)# **no switchport isolate**
Description	The default port is a non-isolated port; Currently, it is not supported to configure the isolation function on aggregation ports and vlan ports.

- Display port optical/copper module information

This command is used to display the information of the optical/copper module inserted on the optical port.

Command	SWITCH#show interface [interface-id] optical-transceiver [info]
Description	If no interface-id is specified, the module information of all ports will be displayed If info is not specified, the DDM information of the port module will be displayed, and if specified, the complete module information (basic information, alarm information, manufacturer information) will be displayed.

2.3. CONFIGURE CASE

- Enter gigabitEthernet0/1 interface configuration mode

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#
```

- Configure the port description information as "TEST_A"

```
SWITCH(config-if)#description TEST_A
```

- Open port enable

```
SWITCH(config-if)#no shutdown
```

- Forced port rate 100M, full duplex, open flow control function

```
SWITCH(config-if)#speed 100
SWITCH(config-if)#duplex full
SWITCH(config-if)#flowcontrol on
```

- Configure the port MTU 1024

```
SWITCH(config-if)#mtu 1024
```

2.4. DISPLAY COMMAND

- Display brief information of all ports

```
SWITCH#show interface brief

--------------------------------------------------------------------------------
Ethernet   Type  Status  Reason  Speed  Duplex  Flowcontrol  Autoneg  Port
Interface                                                             Ch #
--------------------------------------------------------------------------------
GiEO/1     ETH   down    none    --     --      --           --       --
GiEO/2     ETH   up      none    1000M  FULL    OFF          ON       --
GiEO/3     ETH   down    none    --     --      --           --       --
GiEO/4     ETH   down    none    --     --      --           --       --
GiEO/5     ETH   down    none    --     --      --           --       --
GiEO/6     ETH   down    none    --     --      --           --       --
GiEO/7     ETH   down    none    --     --      --           --       --
GiEO/8     ETH   up      none    100M   FULL    OFF          ON       --
GiEO/9     ETH   down    none    --     --      --           --       --
GiEO/10    ETH   down    none    --     --      --           --       --
GiEO/11    ETH   down    none    --     --      --           --       --
GiEO/12    ETH   down    none    --     --      --           --       --
```

- Displays single-port configuration and status information

```
●SWITCH#show interface gigabitethernet0/1
● Interface gigabitethernet0/1
  ● Hardware is eth  current hw addr: 0050.4c82.89a0
  ● Physical:0050.4c82.89a0
  ● Description: test_a
  ● Index 1 metric 0 mtu 1024 speed-unknown duplex-unknown flowcontrol-
unknown
  ● Port mode is invalid
  ● <up>
● vrf binding: not bound
  ● Bandwidth -8
  ● Input packets 0677, bytes 072690,
  ● Multicast packets 0327 broadcast packets 0350 fcs error 00
undersizeerrors 00 oversizeerrors 00
```

- Output packets 00, bytes 00,
- Multicast packets 00 broadcast packets 00

- Display port packet statistics

```
SWITCH#show interface gigabitEthernet0/1 counters
Interface gigabitEthernet16/1
Good Octets Tx          : 1914949
Good Octets Rx          : 0
Bad Octets Rx           : 0
Mac Tx Err Pkts         : 0
Good Packets Tx         : 1913
Good Packets Rx         : 0
Bad Packets Rx          : 0
Broadcast Packet Tx     : 24
Broadcast Packets Rx    : 0
Multicast Packet Tx     : 55
Multicast Packets Rx    : 0
pkts_64_octets          : 285
pkts_65_127_octets      : 263
pkts_128_255_octets     : 42
pkts_256_511_octets     : 36
pkts_512_1023_octets    : 91
pkts_1024_max_octets    : 1196
Excessive Collisions    : 0
UnRecg MAC Cntl Pkts Rx : 0
Flow Ctrl Pkts Sent     : 0
Flow Ctrl Pkts Recvd    : 0
Drop Events             : 0
Undersized Pkts Recvd   : 0
Fragments Recvd         : 0
Oversized Pkts Recvd    : 0
Jabber Pkts Recvd       : 0
mac_rcv_error           : 0
Bad CRC                 : 0
Collisions              : 0
Late Collisions         : 0
Bad Flow Ctrl Recv      : 0
```

- Display port isolation configuration informatio

```
SWITCH#show switchport isolate
interface      config
GiE0/1          isolated
GiE0/2          normal
```

```
GiE0/3          normal
GiE0/4          normal
GiE0/5          normal
GiE0/6          normal
GiE0/7          normal
GiE0/8          normal
GiE0/9          normal
GiE0/10         normal
```

- Display port optical module/copper module DDM information:

DDM information display elements are as follows:

Fields	illustration
Temp	The current operating temperature of the module, in °C, accurate to 1°C.
Voltage	The current working voltage of the module, in V, accurate to 0.01V.
Bias	The current working current of the module, in mA, accurate to 0.01mA.
RX power	The current received optical power of the module, in dBm, accurate to 0.01dBM.
TX power	The current transmit optical power of the module, in dBm, accurate to 0.01dBM.
OK	normal, no intervention required
WARN	Alarm, indicating that the device exceeds the allowable range and needs attention.
ALARM	Abnormal, indicating that the device's allowable state is seriously exceeded and immediate intervention is required.
ABSENT	absent
NA	Port not supported/module not supported
TIMEOUT	Time out
ERR	ERROR

Display single port module DDM information

```
SWITCH#show interface gigabitEthernet0/9 optical-transceiver
  Port       Temp         Voltage        Bias          RX power       TX power
             [C]          [V]            [mA]          [dBm]          [dBm]
------- ---------- ------------- ------------- ------------- -------------
GiE0/9    40(OK)       3.20(OK)       32.34(OK)      -3.98(OK)      1.70(OK)
```

Display all port module DDM information

```
SWITCH#show interface optical-transceiver
  Port       Temp         Voltage        Bias          RX power       TX power
             [C]          [V]            [mA]          [dBm]          [dBm]
------- ---------- ------------- ------------- ------------- -------------
GiE0/9    42(OK)       3.20(OK)       32.34(OK)      -3.98(OK)      1.64(OK)
GiE0/10   ABSENT       ABSENT         ABSENT         ABSENT         ABSENT
GiE0/11   ABSENT       ABSENT         ABSENT         ABSENT         ABSENT
GiE0/12   ABSENT       ABSENT         ABSENT         ABSENT         ABSENT
```

SWITCH#

- Display port optical module/copper module general information:

The overall information display elements of the module are as follows:

Operation error message

Fields	Illustration
Transceiver absent!	Failed to get information, maybe the module is not in place
Get transceiver info timeout!	Timeout to get information, need to get it again
Port doesn't support get module info!	The port does not support getting module information

Basic Information

Fields	Illustration
Transceiver Type	Module Type
Connector Type	Port type
Wavelength(nm)	Wavelength(nm)
Link Length	Supported link lengths
Digital Diagnostic Monitoring	Whether to support DDM function
Vendor Serial Number	Module serial number

Alarm information

Fields	Illustration
RX Channel loss of signal	Received signal loss
RX Channel power high	High received optical power alarm
RX Channel power low	Low received optical power alarm
TX Channel fault	Send Error
TX Channel bias high	Bias current high alarm
TX Channel bias low	Bias current low alarm
TX Channel power high	Sending high optical power alarm
TX Channel power low	Sending low optical power alarm
Temperature high	High temperature alarm
Temperature low	Low temperature alarm
Voltage high	High voltage alarm
Voltage low	Low voltage alarm
None	no alarm
This module doesn't support getting alarm!	The module does not support getting alarm information

Vendor information

Field	Illustration
Vendor Name	Vendor Name
Vendor OUI	Vendor OUI

Vendor Part Number	Vendor Part Number
Vendor Revision	Vendor Revision
Manufacturing Date	Manufacturing Date
Encoding	encoding type

Displays overall information about a single port module

```
SWITCH#show interface gigabitEthernet0/9 optical-transceiver info
#####################################################
                        gigabitEthernet0/9
+-----------------------------------------------+
|Transceiver base information:                  |
+-----------------------------------------------+
|Transceiver Type      :   1000BASE-ZX-SFP      |
|Connector Type        :   LC                   |
|Wavelength(nm)        :   1550                 |
|Link Length       :                            |
|      SMF fiber                                |
|           -- 80km                             |
|Digital Diagnostic Monitoring   : YES          |
|Vendor Serial Number            : WT1703230031 |
+-----------------------------------------------+
|Transceiver current alarm information:         |
+-----------------------------------------------+
|None                                           |
+-----------------------------------------------+
|Transceiver vendor information:                |
+-----------------------------------------------+
|Vendor Name           : OEM                    |
|Vendor OUI            : 000000                 |
|Vendor Part Number    : SFP-GE-ZX-SM1550       |
|Vendor Revision       : V2                     |
|Manufacturing Date    : 2017-03-25             |
|Encoding              : 8B10B                  |
+-----------------------------------------------+
SWITCH#
```

Displays overall information for all port blocks

```
SWITCH#show interface optical-transceiver info
#####################################################
                        gigabitEthernet0/9
+-----------------------------------------------+
|Transceiver base information:                  |
+-----------------------------------------------+
```

```
|Transceiver Type       :    1000BASE-ZX-SFP                  |
|Connector Type         :    LC                               |
|Wavelength(nm)         :    1550                             |
|Link Length        :                                         |
|       SMF fiber                                            |
|             -- 80km                                        |
|Digital Diagnostic Monitoring    : YES                      |
|Vendor Serial Number                 : WT1703230031         |
+--------------------------------------------+
|Transceiver current alarm information:                      |
+--------------------------------------------+
|None                                                        |
+--------------------------------------------+
|Transceiver vendor information:                             |
+--------------------------------------------+
|Vendor Name              : OEM                              |
|Vendor OUI               : 000000                           |
|Vendor Part Number    : SFP-GE-ZX-SM1550                    |
|Vendor Revision        : V2                                 |
|Manufacturing Date    : 2017-03-25                          |
|Encoding                 : 8B10B                            |
+--------------------------------------------+
##############################################################
                          gigabitEthernet0/10
+--------------------------------------------+
|Transceiver base information:                               |
+--------------------------------------------+
|Transceiver Type       :    1000BASE-GT-SFP                 |
|Connector Type         :    Unknown or unspecified          |
|Wavelength(nm)         :    16652                           |
|Link Length        :                                        |
|       Cable Assembly copper                                |
|             -- 100m                                        |
|Digital Diagnostic Monitoring    : NO                       |
|Vendor Serial Number                 : MTC100046            |
+--------------------------------------------+
|Transceiver current alarm information:                      |
+--------------------------------------------+
This module doesn't support getting alarm!
|This module doesn't support getting alarm!                  |
+--------------------------------------------+
|Transceiver vendor information:                             |
```

```
        +-----------------------------------------------+
        |Vendor Name              : OEM                 |
        |Vendor OUI               : 000000              |
        |Vendor Part Number       : SFP-T-CBTX          |
        |Vendor Revision          : F                   |
        |Manufacturing Date       : 2014-10-01          |
        |Encoding                 : 8B10B               |
        +-----------------------------------------------+
        ######################################################
                                gigabitEthernet0/11
        Get result error(Maybe Transceiver absent)!
        ######################################################
                                gigabitEthernet0/12
        Get result error(Maybe Transceiver absent)!
SWITCH#
```

3. CONFIGURE STORM CONTROL

3.1. OVERVIEW OF STORM CONTROL

When there are excessive broadcast, multicast or unknown unicast data streams in the LAN, the network performance will be degraded or even the network will be paralyzed, which is called broadcast storm. Storm control limits the speed of broadcast, multicast and unknown unicast data streams. When the rate of broadcast, unknown name multicast or unknown unicast data streams received by the switch port exceeds the set bandwidth, the device will only allow The data flow of the set bandwidth, the data flow beyond the bandwidth part will be discarded, so as to avoid excessive flooding data flow into the LAN to form a storm.

3.2. CONFIGURE COMMAND

- Configuring interface storm control policies

Command	SWITCH(config-if)#**storm-control** {**broadcast | multicast | unicast | all | unicast-broadcast | multicast-broadcast**} **level** LINE SWITCH(config-if)#**no storm-control**
Description	Configure/delete port storm control policy; Supports selection of configurations in broadcast/multicast/unicast/all/unicast-broadcast/multicast-broadcast, and selection of configurations cannot coexist; Among them, multicast means unknown name multicast packets, and unicast means unknown list broadcast packets; The value of level is the percentage of port bandwidth, which supports adaptive port rate changes.

3.3. CONFIGURE CASE

Case 1: Configure the unknown multicast rate limit on port gigabitEthernet0/1 to 10% of the total bandwidth.

- Enter gigabitEthernet0/1 interface configuration mode:

```
SWITCH#
SWITCH#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#
```

- Configure the interface unknown name multicast rate limit policy:

```
SWITCH(config-if)#storm-control multicast level 10
```

3.4. DISPLAY COMMAND

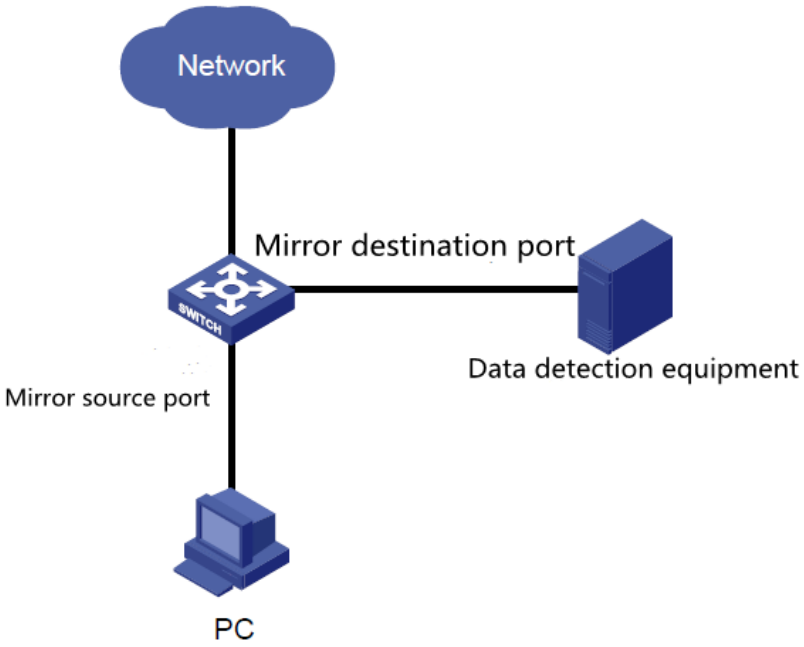
- Display all port storm control configuration

```
SWITCH#show storm-control
Port        BcastLevel     McastLevel     Unicastlevel
GiE0/1      100.00%          10.00%       100.00%
GiE0/2      100.00%        100.00%        100.00%
GiE0/3      100.00%        100.00%        100.00%
GiE0/4      100.00%        100.00%        100.00%
GiE0/5      100.00%        100.00%        100.00%
GiE0/6      100.00%        100.00%        100.00%
GiE0/7      100.00%        100.00%        100.00%
GiE0/8      100.00%        100.00%        100.00%
GiE0/9      100.00%        100.00%        100.00%
GiE0/10     100.00%        100.00%        100.00%
GiE0/11     100.00%        100.00%        100.00%
GiE0/12     100.00%        100.00%        100.00%
```

4. CONFIGURE SPAN

4.1. SPAN OVERVIEW

SPAN (Local Switched Port Analyzer) is a local mirroring function. The SPAN function copies the packets of the specified port to the destination port. Generally, the SPAN destination port is connected to a data detection device. Users can use these devices to analyze the packets received by the destination port for network monitoring and troubleshooting.



SPAN does not affect the packet exchange between the source port and the destination port, but only copies all incoming and outgoing packets of the source port to the destination port. When the mirrored traffic of the source port exceeds the bandwidth of the destination port, for example, the 100Mbps destination port monitors the traffic of the 1000Mbps source port, the packets may be discarded.

Based on session management, SPAN configures the source port and destination port of SPAN in the session. In a session, there can only be one destination port, but multiple source ports can be configured at the same time.

4.2. CONFIGURE COMMAND

- Create a session

Command	SWITCH(config)#**monitor session** SESSION-ID SWITCH(config)#**no monitor session** SESSION-ID
Description	Create/delete a session, create a session and enter session mode at the same time; 7 sessions supported

- Configure the session descriptor

Command	SWITCH(config-monitor)#**description** DESC
Description	configure session descriptor

- Configure the source port

Command	SWITCH(config-monitor)#**source interface** IFNAME {**both | rx | tx**} SWITCH(config-monitor)#**no source interface** IFNAME {**both | rx | tx**}
Description	Create/Delete SPAN Source Port

- Configure the destination port

Command	SWITCH(config-monitor)#**destination interface** IFNAME SWITCH(config-monitor)#**no destination interface** IFNAME
Description	Create/Delete SPAN destination port

4.3. CONFIGURE CASE

Case 1: Use port gigabitEthernet0/8 to monitor the ingress packets of gigabitEthernet0/1 and the egress/ingress packets of gigabitEthernet0/2. The monitoring session name is defined as "TRAFFIC_MONITOR".

- Enter global mode and establish a session:

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#monitor session 1
SWITCH(config-monitor)#
```

- Configure the session description information as "TRAFFIC_MONITOR"

```
SWITCH(config-monitor)#description TRAFFIC_MONITOR
```

- Configure the session source port

```
SWITCH(config-monitor)#source interface gigabitEthernet0/1 rx
SWITCH(config-monitor)#source interface gigabitEthernet0/2 both
```

- Configure the session destination port

```
SWITCH(config-monitor)#destination interface gigabitEthernet0/8
```

4.4. DISPLAY COMMAND

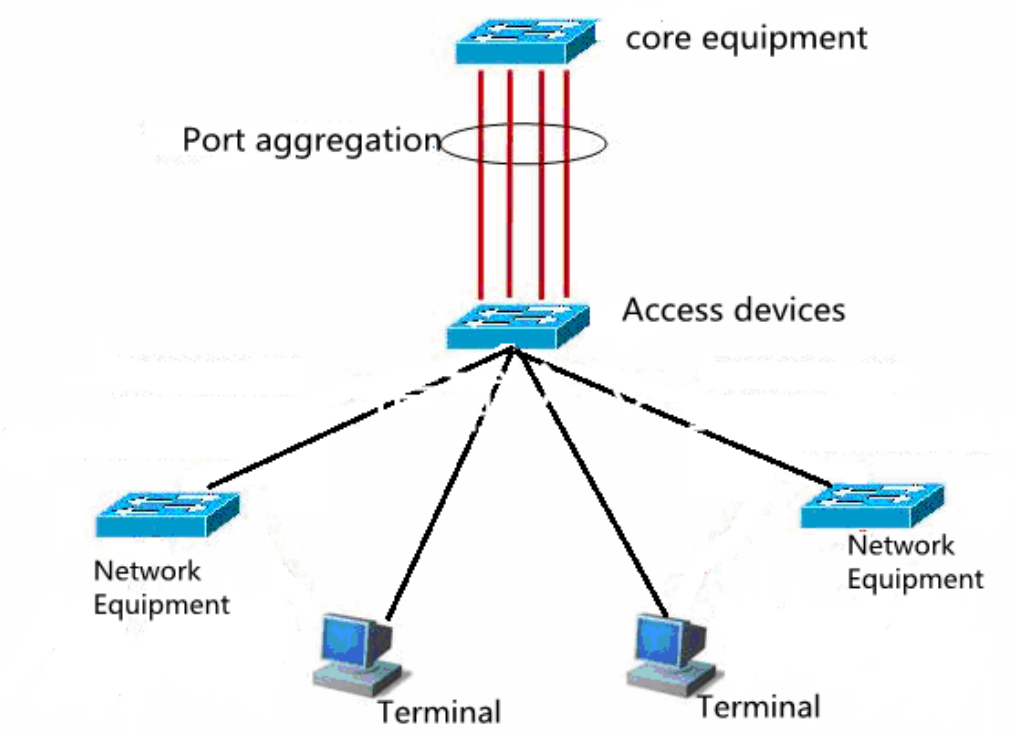
- Display concrete session:

```
SWITCH#show  monitor session 1
session 1
---------------
description       : TRAFFIC_MONITOR
type              : local
source intf       :
    tx            : gigabitEthernet0/2
    rx            : gigabitEthernet0/1  gigabitEthernet0/2
    both          : gigabitEthernet0/2
source VLANs      :
    rx            :
destination ports : gigabitEthernet0/8
Legend: f = forwarding enabled, l = learning enabled
```

5. CONFIGURE PORT AGGREGATION

5.1. OVERVIEW OF AGGREGATE PORT

Bundle multiple physical links together to create a logical link, which we call an aggregation port (port-channel, the latter PO port), and this function is called a port aggregation function. The aggregation port function conforms to the IEEE802.3ad standard. It can be used to expand the link bandwidth and provide higher connection reliability. It is often used for port uplinks, as shown in the figure below.

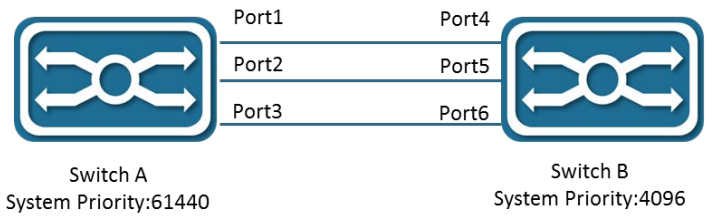


The aggregate port has the following characteristics: high bandwidth, the total bandwidth of the aggregate port is the sum of the bandwidth of the physical member ports; supports traffic balancing policies, which can distribute traffic to each member link according to the policy; supports link backup, when one of the aggregate ports When a member link is disconnected, the system will automatically distribute the traffic of the member link to other valid member links in the aggregate port.

5.2. LACP OVERVIEW

LACP (Link Aggregation Control Protocol, Link Aggregation Control Protocol) based on the IEEE802.3ad standard is a protocol for realizing dynamic link aggregation. If the port enables the LACP protocol, the port will send LACPDU to announce its system priority, system MAC, port priority, port number and operation key, etc. After the connected device receives the LACP message from the peer end, it compares the system priorities of the two ends according to the system ID in the message. On the side with the higher system ID priority, the ports in the aggregation group are set to be in the aggregation state according to the order of port ID priority from high to low, and the updated LACP packet is sent out. The corresponding port will also be set to the aggregation state, so that the two sides can reach the same agreement when the port exits or joins the aggregation group. The physical link can forward data packets only after the ports on both sides have completed the dynamic aggregation and binding operation.

After the LACP member interface link is bound, periodic LACP packet exchange will be carried out. When no LACP packet is received for a period of time, it is considered that the packet reception timed out, the member interface link is unbound, and the port is in a state of non-forwarding again. state. There are two modes of timeout here: long timeout mode and short timeout mode. In long timeout mode, the port sends a packet every 30 seconds. In the short timeout mode, the port sends a packet every 1 second. If the port does not receive a packet from the peer for 3 seconds, it is in the packet receiving timeout.



As shown in the figure above, Switch A and Switch B are connected together through 3 ports. Set the system priority of switch A to 61440, and set the system priority of switch B to 4096. Enable LACP link aggregation on the three directly connected ports of switches A and B, set the aggregation mode of the three ports to active mode, and set the port priority of the three ports to the default priority of 32768.

After receiving the LACP message from the peer, switch B finds that its system ID has a higher priority (switch B has a higher system priority than switch A), so it follows the order of port ID priority (in the

case of the same port priority) , in the order of port numbers from small to large) to set ports 4, 5, and 6 to be in the aggregation state. After switch A receives the updated LACP packet from switch B, it finds that the peer's system ID has a higher priority, and sets the port to the aggregation state, and also sets the ports 1, 2, and 3 to the aggregation state.

5.3. CONFIGURE COMMAND

- Port join/exit aggregate port

Command	Add static aggregation port: SWITCH(config-if)#**channel-group** ID **mode manual** Join Dynamic Aggregation (LACP): SWITCH(config-if)#**channel-group** ID **mode** {**active** | **passive**} Exit the aggregation port: SWITCH(config-if)#**no channel-group**
Description	Support 12 aggregation ports <1-12>; An aggregate port is either static or dynamic, determined by the joining method of the first member port added. Active aggregation mode means that the port will actively initiate LACP aggregation operations; Passive aggregation mode means that the port will not actively initiate LACP aggregation operations, but will passively participate in LACP calculations after receiving LACP packets from neighbors.

Illustration

✦ When the aggregation port (PO port) is not created and the first port is added to the aggregation port, the PO port will be created actively, and the default attribute of the PO port is the port attribute;

✦ When a port is added to an aggregation port, the following basic attributes are required to be the same as that of the aggregation port:

Port VLAN attribute configuration;

Port isolation configuration.

- Configure the LACP system priority

Command	SWITCH(config)#**lacp system-priority** SYSTEM-PRIORITY SWITCH(config)#**no lacp system-priority**
Description	The system priority range is <1-65535>, the default is 32768. All dynamic link groups of a device can only have one LACP system priority. Modifying this value will affect all aggregation groups on the switch.

- Configure LACP port priority

Command	SWITCH(config-if)#**lacp port-priority** PORT-PRIORITY SWITCH(config-if)#**no lacp port-priority**
Description	Port priority is configured in interface mode, only physical port configuration is supported. Port priority range is <1-65535>, default is 32768.

- Configure LACP timeout mode:

command	SWITCH(config-if)#**lacp timeout {long | short}** SWITCH(config-if)#**no lacp timeout**
Description	Port priority is configured in interface mode, only physical port configuration is supported. The default is long mode, LACP protocol packet sending interval is 30S, 90S timeout; short mode, LACP protocol packet sending interval is 1S, 3S timeout.

- Configure the load balancing mode

Command	SWITCH(config)#**port-channel load-balance** {**dst-ip | dst-mac | dst-port | src-dst-ip | src-dst-mac | src-dst-port | src-ip | src-mac | src-port**} SWITCH(config)#**no port-channel load-balance**
Description	Configure load balancing mode, default src-dst-mac

5.4. CONFIGURE CASE

- Case requirements：configure gigabitEthernet0/5、gigabitEthernet0/6 add po1； Configure the load balancing mode as src-ip.
- Adding an Aggregate Port on an Interface：

```
SWITCH(config)#interface gigabitEthernet0/5
SWITCH(config-if)#channel-group 1 mode manual
```

```
SWITCH(config-if)#exit
SWITCH(config)#interface gigabitEthernet0/6
SWITCH(config-if)#channel-group 1 mode manual
SWITCH(config-if)#exit
SWITCH(config)#port-channel load-balance src-ip
```

5.5. DISPLAY COMMAND

- Display aggregate port configuration and status information

```
SWITCH#show port-channel
Load balance: Source and Destination Mac address

Interface po3
  Type: static
  Member:
    gigabitEthernet0/18     link down     Disable

Interface po8
  Type: LACP
  Member:
    gigabitEthernet0/19     link up       Enable
    gigabitEthernet0/17     link up       Enable

SWITCH#show port-channel 8
Interface po8
  Type: LACP
  Member:
    gigabitEthernet0/19     link up       Enable
    gigabitEthernet0/17     link up       Enable

SWITCH#show port-channel load-balance
Source and Destination Mac address
```

- Display LACP information

```
SWITCH#show lacp summary
% Aggregator po8 1008
% Aggregator Type: Layer2
% Admin Key: 0008 - Oper Key 0008
%   Link: gigabitEthernet0/17 (17) sync: 1 status: Bundled
%   Link: gigabitEthernet0/19 (19) sync: 1 status: Bundled

SWITCH#show lacp detail
% Aggregator po8 1008
```

```
% Aggregator Type: Layer2
%  Mac address: 74:b9:eb:ee:25:46
%  Admin Key: 0008 - Oper Key 0008
%  Actor LAG ID- 0x8000,74-b9-eb-ee-25-46,0x0008
%  Receive link count: 2 - Transmit link count: 2
%  Individual: 0 - Ready: 1
%  Partner LAG ID- 0x8000,00-01-a0-00-10-10,0x0032
%   Link: gigabitEthernet0/17 (17) sync: 1 status: Bundled
%   Link: gigabitEthernet0/19 (19) sync: 1 status: Bundled

SWITCH#show lacp 8
% Aggregator po8 1008 Admin Key: 0008 - Oper Key 0008
% Partner LAG ID: 0x8000,00-01-a0-00-10-10,0x0032
% Partner Oper Key 0050

SWITCH#show lacp sys-id
% System 8000,74-b9-eb-ee-25-46

SWITCH#show lacp port gigabitEthernet0/19
% LACP link info: gigabitEthernet0/19 - 19
% LAG ID: 0x8000,74-b9-eb-ee-25-46,0x0008
% Partner oper LAG ID: 0x8000,00-01-a0-00-10-10,0x0032
% Actor Port priority: 0x8000 (32768)
% Admin key: 0x0008 (8) Oper key: 0x0008 (8)
% Physical admin key:(1)
% Receive machine state : Current
% Periodic Transmission machine state : Slow periodic
% Mux machine state : Collecting/Distributing
% Oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Partner oper state: ACT:1 TIM:0 AGG:1 SYN:1 COL:1 DIS:1 DEF:0 EXP:0
% Partner link info: admin port 0
% Partner oper port: 20
% Partner admin LAG ID: 0x0000-00:00:00:00:0000
% Admin state: ACT:1 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner admin state: ACT:0 TIM:0 AGG:1 SYN:0 COL:0 DIS:0 DEF:1 EXP:0
% Partner system priority - admin:0x0000 - oper:0x8000
% Partner port priority - admin:0x0000 - oper:0x8000
% Aggregator ID: 1008
```

- Display aggregate port information

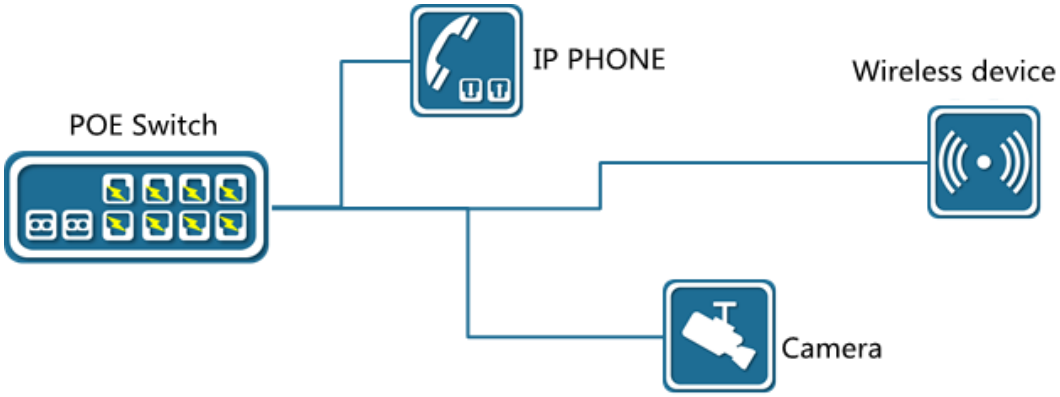
```
SWITCH#show int po8
Interface po8
```

```
  Hardware is AGG  Current HW addr: 74b9.ebee.2546
  Logical:(not set)
  Port Mode is access
  interface configure:
    medium-fiber mtu 1526 speed-auto duplex-auto flowcontrol-off
autonego-off
  interface status:
    link-up bandwidth-2g
  Aggregate Members:(LACP)
    gigabitEthernet0/19     link up       Enable
    gigabitEthernet0/17     link up       Enable
  input packets:
    Good Octets Rx          : 18986
    Good Packets Rx         : 104
    Broadcast Packets Rx    : 0
    Multicast Packets Rx    : 104
  ouput packets:
    Good Octets Tx          : 38529
    Good Packets Tx         : 359
    Broadcast Packet Tx     : 4
    Multicast Packet Tx     : 355
  un-normal packets:
    Drop Events             : 0
    Undersized Pkts Recvd   : 0
    Oversized Pkts Recvd    : 0
   Bad CRC                 : 0
```

6. CONFIGURE POE

6.1. POE OVERVIEW

Power over Ethernet, or PoE for short, is a technology that can provide DC power supply while exchanging data with the terminal through twisted pair cables in the Ethernet circuit. It is commonly used to supply power to Internet phones, WIFI APs, network cameras, hubs, computers and other equipment. According to the standard, the longest power supply distance is 100m.



PSE (Power Sourcing Equipment, power supply equipment), such as the PoE switch in the figure above. The PSE finds and detects PDs on the lines of the PoE ports, classifies the PDs, and supplies power to them. When it is detected that the PD is unplugged, the PSE stops supplying power. PD is a device that receives power from PSE, such as IP phone, wireless device, and camera in the above picture.

PoE development has gone through two sets of standards:

IEEE 802.3af (15.4W) is the first PoE power supply standard, which specifies the power over Ethernet standard and is the mainstream implementation standard for PoE applications. It specifies power detection and control in remote systems, and specifies how routers, switches, and hubs can power devices such as IP phones, security systems, and wireless LAN access points through Ethernet cables. IEEE802.3at (25.5W) was born in response to the needs of high-power terminals. On the basis of being compatible with 802.3af, it provides greater power supply requirements and meets new needs. According to the IEEE 802.3af specification, the PoE power consumption on a powered device (PD) is limited to 12.95W. IEEE 802.3at, which defines devices with power requirements higher than 12.95W as Class 4 (this class is described in IEEE 802.3af but reserved for future use), can extend the power level to 25W or higher.

6.2. CONFIGURE COMMAND

- Configure external power supply

command	SWITCH(config)#**poe powersupply** POWER SWITCH(config)#**no poe powersupply**
Description	Configure external power The default power calculation method: the product of the number of PoE power supply ports and the single port 15.4W If the configured power is less than the current power consumption of the device, power off the PD device on the port with the lower priority, and the port priority is a higher priority with a smaller port ID.

- Configure the port power supply enable

Command	SWITCH (config-if)#**poe enable** SWITCH (config-if)#**no poe enable**
Description	Configure the port to enable power supply Default port power supply enabled

- Configuration enable compatibility mode

Command	SWITCH (config)#**poe legacy** SWITCH (config)#**no poe legacy**
Description	Configuring PoE Globally to Enable or Disable Compatibility Mode Using this command on a port that is not connected to a PD device may cause the peer device to be burned by wrong power-on. Please make sure that the port uses this command when connecting to a PD device. For non-standard PoE devices, the Class rating is uniformly displayed as 0

6.3. CONFIGURE CASE

Case 1: Configure port gigabitEthernet0/1 to enable power supply

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#poe enable
```

6.4. DISPALY COMMAND

- Display PoE system power supply information

```
SWITCH#show poe powersupply
  Power supply                : 123.2W
  Power consume            : 44.1W
  Power management     : energy-saving
```

```
  Disconnect mode          : DC
  Powered ports              : 2
```

- Display PoE port power supply information

```
SWITCH#show poe interfaces
Interface   enable  status  reason      class  icut(mA) power(W)
-------------------------------------------------------------------
GiE0/1      YES     OFF     short       4      --       --
GiE0/2      YES     OFF     --          -      --       --
GiE0/3      YES     OFF     --          -      --       --
GiE0/4      YES     OFF     --          -      --       --
GiE0/5      YES     OFF     --          -      --       --
GiE0/6      YES     ON      --          4      270.2    14.0
GiE0/7      YES     OFF     --          -      --       --
GiE0/8      YES     OFF     --          -      --       --
```

7. CONFIGURE VLAN

7.1. VLAN FUNCTION OVERVIEW

VLAN is the abbreviation of Virtual Local Area Network (Virtual Local Area Network), which is a logical network divided on a physical network. This network corresponds to the second layer network of the ISO model. The division of VLANs is not limited by the actual physical location of the network ports. A VLAN has the same properties as a normal physical network, except that there is no physical location restriction, it is the same as a normal LAN. Layer 2 unicast, broadcast, and multicast frames are forwarded and flooded within a VLAN without directly entering other VLANs.

Port-based VLAN is the simplest VLAN division method. Users can divide the ports on the device into different VLANs, and then the packets received from a certain port can only be transmitted in the corresponding VLAN, so as to realize the isolation of broadcast domains and the division of virtual work groups.

The port link types of Ethernet switches can be divided into three types: Access, Trunk, and Hybrid. These three ports will be processed differently when they join VLAN and forward packets.

Access type：Ports can only belong to 1 VLAN; generally used for connections between switches and end users；

Trunk type：Ports can belong to multiple VLANs, and can receive and send packets of multiple VLANs, but only native VLANs can be untagged; generally used for connections between switches;

Hybrid type：The port can belong to multiple VLANs, can receive and send packets of multiple VLANs, and can configure whether the relevant VLANs are tagged with VLANs according to the user's needs; it can be used for connection between switches, or for connecting users' computers.

7.2. CONFIGURE COMMAND

- Create delete VLAN

command	SWITCH(config)#**vlan** VLAN_RANGE SWITCH(config)#**no vlan** VLAN_RANGE
Description	create/delete VLAN

- Configure the VLAN based on the access port

command	SWITCH(config)#**interface** IFNAME SWITCH(config-if)#**switchport mode access**
Description	Enter Ethernet port mode. Configure the port type as an Access port (by default, the port is an Access port).

command	SWITCH(config-if)#**switchport access vlan** VLANID SWITCH(config-if)#**no switchport access vlan**
Description	Add the current port to the specified VLAN (by default, all access ports belong to and only belong to VLAN1). The no command returns to the default. The above command can be used only when the interface has been configured as an access port, and the specified VLAN must have been created. After the configuration is not VLAN1, if the corresponding VLAN is deleted, it will be automatically restored to VLAN1.

- Configure VLAN based on trunk port

Command	SWITCH(config)#**interface** IFNAME SWITCH(config-if)#**switchport mode trunk**
Description	Enter Ethernet port mode. Configure the port type trunk port.

Command	SWITCH(config-if)#**switchport trunk allowed vlan** { **all** | VLAN_LIST | **none**} SWITCH(config-if)#**no switchport trunk allowed vlan** VLAN_LIST
Description	Maintains the Allowed VLAN list of the trunk port. The above command can be used only when the interface has been configured as a trunk port. All means automatic mode, which automatically joins all created VLANs (even if it is subsequently created, it will be automatically added); None means to clear the Allowed VLAN list, that is, the port does not belong to any VLAN (including native vlan); VLAN_LIST means to manually set the Allowed VLAN list. If it belongs to ALL (automatic mode) before, the Allowed VLAN list will be cleared first, and then the VLAN list will be added. VLAN_LIST supports standard multi-vlan representation methods ("-" and "," and combinations of both); When the no keyword is added in front, it means that the VLAN indicated by VLAN_LIST is deleted from the Allowed VLAN list.

	When setting all, change the maintenance of the Allowed VLAN list to automatic mode, and change other commands to manual mode. (By default, it is in automatic mode, and when it is switched from other port mode to trunk port, it is in automatic mode). Only created VLANs can be added to the Allowed VLAN list; when a VLAN is deleted, the corresponding VLAN in the Allowed VLAN list will be automatically deleted.

Command	SWITCH(config-if)#**switchport trunk native vlan** VLANID SWITCH(config-if)#**no switchport trunk native vlan**
Description	Set the native vlan of the trunk port. (By default, the native VLAN of the trunk port is VLAN1.) The no command restores the default value. The above command can be used only when the interface has been configured as a trunk port. The setting of the Native VLAN has nothing to do with whether the Allowed VLAN contains this VLAN, or even whether the VLAN is created, that is, the native VLAN can be set to a VLAN that has not been created.

Illustration

✦The default VLAN ID of the trunk port of the local device must be the same as the default VLAN ID of the trunk port of the connected device, otherwise the packets of the default VLAN will not be transmitted correctly.

- Configuring VLAN based on Hybrid port

command	SWITCH(config)#**interface** IFNAME SWITCH(config-if)#**switchport mode hybrid**
Description	Enter Ethernet port mode. Configure the port type Hybrid port

Command	SWITCH(config-if)#**switchport hybrid allowed vlan** { **all** | VLAN_LIST | **none**} SWITCH(config-if)#**no switchport hybrid allowed vlan** VLAN_LIST
Description	Maintains the Allowed VLAN list of the Hybrid port. The above command can be used only when the interface has been configured as a hybrid port. All means automatic mode, which automatically joins all created VLANs (even if it is subsequently created, it will be automatically added);

	None means to clear the Allowed VLAN list, that is, the port does not belong to any VLAN (including native vlan); VLAN_LIST means to manually set the Allowed VLAN list. If it belongs to ALL (automatic mode) before, the Allowed VLAN list will be cleared first, and then the VLAN list will be added. VLAN_LIST supports standard multiple VLAN representation methods ("-" and "," and combinations of both); When the no keyword is added in front, it means that the VLAN indicated by VLAN_LIST is deleted from the Allowed VLAN list. When setting all, change the maintenance of the Allowed VLAN list to automatic mode, and change other commands to manual mode. (By default, it is in automatic mode, and when it is switched from other port mode to trunk port, it is in automatic mode). Only created VLANs can be added to the Allowed VLAN list; when a VLAN is deleted, the corresponding VLAN in the Allowed VLAN list will be automatically deleted.

Command	SWITCH(config-if)#**switchport hybrid vlan** VLANID SWITCH(config-if)#**no switchport hybrid vlan**
Description	Set the default VLAN of the Hybrid port (when the port receives untagged packets, the default VLAN is specified; the packets carrying the default VLAN are output untaged), (by default, the default VLAN of the port is VLAN1), the no command is restored to the default. The above command can be used only when the interface has been configured as a hybrid port. The setting of the default VLAN has nothing to do with whether the Allowed VLAN includes this VLAN, or even whether the VLAN is created, that is, the default VLAN can be set to a VLAN that has not been created.

Command	SWITCH(config-if)#**switchport hybrid untagged vlan** VLAN_LIST SWITCH(config-if)#**no switchport hybrid untagged vlan** VLAN_LIST
Description	Maintains the untagged VLAN list of the Hybrid port. (Because the default VLAN must be untagged output, therefore, it is not maintained by the untagged VLAN list. By default, the untagged VLAN list is empty, that is, except the default VLAN, all other VLANs are tagged and output).

	The VLANs maintained in the Untagged VLAN list must be in the Allowed VLAN list of the Hybird port. Therefore, when a VLAN is deleted from the Allowed VLAN, it will also be deleted from the Untagged VLAN list. Since the untagged VLAN list does not maintain the default VLAN, if a VLAN in the previous list is set as the default VLAN, it will be deleted from the untagged VLAN list, and the process is irreversible.

Illustration:

✦The default VLAN ID of the hybrid port of the local device must be the same as the default VLAN ID of the hybrid port of the connected device, otherwise the packets of the default VLAN will not be transmitted correctly.

7.3. DISPLAY COMMAND

- In privileged mode, you can view VLAN information. The displayed information includes VLAN VID, VLAN status, VLAN member ports, and VLAN configuration information.
- Display VLAN

```
VLAN ID  Name         State   H/W Status  Member ports
                                          (u)-Untagged, (t)-Tagged
======= ============ ======= =========== ============================
1        default      ACTIVE  Up          gigabitEthernet0/2(u)
                                             gigabitEthernet0/3(u)
```

8. CONFIGURE QINQ

8.1. QINQ OVERVIEW

QinQ technology (also known as Stacked VLAN or Double VLAN). The standard comes from IEEE 802.1ad, which means that the public network VLAN Tag of a service provider network is encapsulated before the user packet enters the service provider network, and the private network user VLAN Tag in the user packet is regarded as data, so that the packet carries Two layers of VLAN tags traverse the service provider network.

In the metropolitan area network, a large number of VLANs are required to isolate users, and the 4094 VLANs supported by the IEEE 802.1Q protocol are far from meeting the requirements. Through the double-layer Tag encapsulation of QinQ technology, in the service provider network, the packets are only transmitted according to the unique outer VLAN Tag allocated on the public network, so that the VLANs of different private network users can be reused, and the number of VLAN tags available to users is expanded. At the same time, it provides a simple Layer 2 VPN function, so QINQ technology is actually a VLAN VPN technology.

In addition to QINQ, common VLAN VPN technologies include VLAN Mapping. The only difference between the two is that QINQ is for stacking VLANs, and VLAN Mapping is for VLAN mapping.

- VLAN Stacking: From the user network to the provider network, a single-layer tag becomes a double-layer tag, and the C-Tag remains in the packet as an inner-layer tag; in the reverse direction, it changes from a double-layer tag to a single-layer tag.
- VLAN Mapping: From the user network to the provider network, it is still a single-layer Tag, but the C-Tag becomes an S-Tag; in the reverse direction, the S-Tag becomes a C-Tag.

8.2. CONFIGURATION ILLUSTRATION

QINQ is divided into three categories：

- A：Basic QINQ is enabled and disabled based on the interface. When an interface with basic QINQ enabled receives a packet, it is treated as an untag packet. On the basis of the original packet, a VLAN tag of the default VLAN of the port is added.
- B：Flexible QINQ based on C-tag, according to the C-VLAN Tag on the user side, according to the configured mapping policy, add a layer of S-VLAN Tag on the basis of the original packet. There are two optional configuration methods for this type of QINQ, and only one of them can be selected. One way is to configure the mapping relationship between C-VLAN and S-VLAN directly on the interface; the other way is to configure VLAN VPN globally (which includes the mapping

relationship between C-VLAN and S-VLAN), and then associate the VPN on the interface. When using the same mapping policy for multiple interfaces, generally choose the latter configuration method. For this type of QINQ, if the packets received by the interface are untagged, the C-tag is the default VLAN Tag of the interface.

- C：ACL-based flexible QINQ, according to the configured flow policy, to add outer tags. The configuration of this type of QINQ is placed in the "QOS" module. For details, please refer to the "Configuring QOS" chapter. The policy pair between Policy-map and Class-map: "nest vlan<1-4094>" is used to configure ACL-based Flexibl

The above three types of QINQs can be enabled on the same port at the same time, and their priority relationship is: Type C > Type B > Type A.

VLAN Mapping is divided into 1:1 VLAN Mapping and 1:N VLAN Mapping (the reverse is N:1). Currently, only 1:1 VLAN Mapping is supported. VLAN Mapping is configured by configuring VLAN VPN globally, and then associating VPN on interface. VLAN Mapping takes effect only for tagged packets, which is very different from the QINQ function.

When configuring the QINQ and VLAN Mapping functions, pay attention to the following points:

□● Only physical interfaces support the configuration of QINQ and VLAN Mapping, but not on aggregated interfaces.

□● VLAN Mapping takes effect only for tagged packets. Upstream, original packets must carry tags to implement CVLAN-to-SVLAN mapping; for downstream, the VLAN output rule on downlink interfaces must be tag output to implement SVLAN-to-SVLAN mapping. Mapping of CVLANs.

□● When using the QINQ function or the VLAN Mapping function, it needs to be used in conjunction with the VLAN configuration. In the input and output direction, the filtering function of the VLAN, and the rules for whether the VLAN carries a tag are all subject to the VLAN configuration.

Specific requirements are as follows：

- ▷ Both CVLAN and SVLAN need to be added to the allow list of the downlink interface (connected to the Customer network), otherwise the flow will be filtered;
- ▷ SVLAN needs to be added to the allow list of the uplink interface (connected to the Provider network), otherwise the flow will be filtered;

▷ For QINQ, on the downlink interface, SVLAN should be configured with untag output, so as to strip the outer tag of QINQ downstream;

▷ For VLAN-Map, since it is only valid for untag packets, the SVLAN should be configured with tag output for the downlink interface, otherwise the downstream flow cannot complete the mapping from SVLAN to CVLAN.

- The globally configured VLAN VPN is either used for VLAN Stacking (QINQ) or VLAN Mapping, but cannot be used for both at the same time.
- VLAN Mapping only supports 1:1 mapping. Therefore, if there are VLAN VPNs with N:1 mapping, they cannot be associated with the interface as the VPN of VLAN mapping. Similarly, if the VPN has been associated with the interface as the VLAN mapping, the mapping relationship Cannot be changed to N:1.
- The mapping relationship of VLAN Mapping must be consistent globally. Therefore, different interfaces can only be associated with the same VLAN VPN.
- On the same interface, if you need to apply VLAN Mapping and QINQ at the same time, it should be noted that the two functions need to control different CVLANs and SVLANs.

The specific constraints are as follows:

▷ If VLAN Mapping is used together with basic QINQ, the basic QINQ will take effect and VLAN Mapping will be invalid.

▷ If VLAN Mapping and flexible QINQ are used together, if a flow passes through the SVLAN mapped by VLAN Mapping and can be used as a CVLAN to match the mapping policy of flexible QINQ, then the final packet will take effect with flexible QINQ, adding SVLAN as external Layer TAG, the inner layer TAG remains unchanged (not the VLAN mapped by VLAN Mapping).

▷ Because of the above constraints, when two applications are enabled on the same interface, it is necessary to pay attention to the fact that the VLANs controlled by the two do not overlap. invalid.

- For the B-type QINQ, you can either choose to configure the mapping policy directly under the interface, or choose to associate with the VPN, but cannot be configured at the same time.

8.3. CONFIGURE COMMAND

- Create /delete VLAN VPN

command	SWITCH(config)#**vlan-vpn** VPN-NAME SWITCH(config)#**no vlan-vpn** VPN-NAME

Description	There can be multiple VPNs in the system, and each VPN maintains the mapping relationship between independent CVLANs and SVLANs. A VPN will only actually take effect when applied to an interface. A VPN can be applied to VLAN Stacking (QINQ) or VLAN Mapping, but only one of the two can be selected.

- Add/delete VPN mapping relationship

Command	SWITCH(config-vlan-vpn)#**cvlan** VLAN_LIST **svlan** VLANID SWITCH(config-vlan-vpn)#**no cvlan** VLAN_LIST SWITCH(config-vlan-vpn)#**no cvlan**
Description	The valid range of VLAN_LIST and VLANID is <1,4094>, VLAN_LIST supports standard multi-vlan representation method ("-" and "," and combination of both). No cvlan without any parameters, clears all the mapping relationships in the VPN.

- Configure/cancel basic QINQ

Command	SWITCH(config-if)#**switchport vlan-stacking basic** SWITCH(config-if)#**no switchport vlan-stacking basic**
Description	After basic QINQ is enabled, all incoming packets from this interface match the QINQ rules, and the mapped SVLAN is the default VLAN ID of the interface.

- Add/delete the mapping relationship of QINQ under the interface

Command	SWITCH(config-if)#**switchport vlan-stacking cvlan** VLAN_LIST **svlan** VLANID SWITCH(config-if)#**no switchport vlan-stacking cvlan** VLAN_LIST SWITCH(config-if)#**no switchport vlan-stacking cvlan**
Description	It is similar to the mapping relationship configuration under VPN. You can directly configure the mapping relationship only when the interface is not associated with a VPN.

- Interface association/disassociation with QINQ VPN

Command	SWITCH(config-if)#**switchport vlan-stacking vpn** VPN-NAME SWITCH(config-if)#**no switchport vlan-stacking vpn**
Description	An interface can only be associated with one VPN. Only when the interface is not configured with a mapping relationship, the VPN association configuration can be performed.

- Cancel all QINQ configurations on the interface

Command	SWITCH(config-if)#**no switchport vlan-stacking**
Description	Equivalent to no switchport vlan-stacking basic no switchport vlan-stacking cvlan no switchport vlan-stacking vpn The three commands.

- Interface association/disassociation VLAN Mapping VPN

Command	SWITCH(config-if)#**switchport vlan-mapping vpn** VPN-NAME SWITCH(config-if)#**no switchport vlan-mapping**
Description	VLAN mapping configured on different interfaces must be associated with the same VPN. And the mapping relationship in the corresponding VPN must be 1:1.

8.4. CONFIGURE CASE

Case 1: Implementing Layer 2 VPN services based on ports

Service Provider provides VPN for Enterprise A and Enterprise B:

- Enterprise A and enterprise B belong to different VLANs on the public network, and communicate through their own public network VLANs.
- The VLANs in enterprise A and enterprise B are transparent to the public network, and the user VLANs in enterprise A and enterprise B can be reused without conflict.

- Tunnel will encapsulate a layer of VLAN Tag of Native VLAN to user data packets. In the public network, user data packets are transmitted in the native VLAN, which does not affect the use of VLANs in different enterprise user networks, and implements a simple Layer 2 VPN.

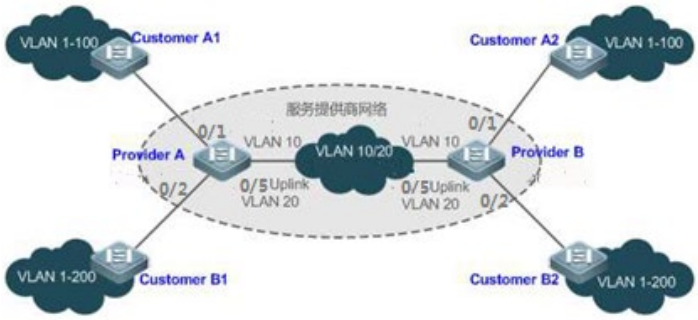


illustration:

- Customer A1, Customer A2, Customer B1 and Customer B2 are the edge devices of the network where enterprise user A and enterprise user B reside, respectively. Provider A and Provider B are edge devices of the service provider network, and Enterprise A and Enterprise B access the public network through the edge devices of the provider.
- The VLAN range of the office network used by enterprise A is VLAN 1-100.
- The VLAN range of the office network used by enterprise B is VLAN 1-200.

ProviderA and ProviderB are completely symmetrical, and the configurations are exactly the same:

- Configure VLAN

```
SWITCH(config)#vlan 2-200
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 1-100
SWITCH(config-if)#switchport trunk native vlan 10
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk native vlan 10
SWITCH(config-if)#interface gigabitEthernet0/5
SWITCH(config-if)#switchport mode trunk
```

- Configure basic QINQ

```
SWITCH(config)#interface gigabitEthernet0/1-2
SWITCH(config-if)#switchport vlan-stacking basic
SWITCH(config-if)#exit
```

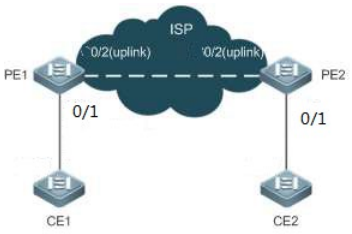
Case 2: Flexible QINQ based on C-Tag to implement Layer 2 VPN and service flow management

Basic QinQ can only encapsulate user data packets in the outer tag of a native VLAN, that is, the encapsulation of the outer tag depends on the native VLAN of the tunnel port. Flexible QinQ provides flexible encapsulation of external tags (S-Tags) of service providers (ISPs) according to the tags (C-Tags) of user packets, so as to flexibly implement VPN transparent transmission and service flow QoS policies.

- Broadband Internet access and IPTV services are important parts of the services carried by the metropolitan area network. The metropolitan area network service provider network divides VLANs for different service flows to differentiate management, and provides QoS policy services for these VLANs. On the edge device of the service provider, QinQ based on C-Tag can be used to encapsulate the relevant VLAN of the user's service flow, and the QoS policy of the service provider's network can be used for guaranteed transmission while transparent transmission.
- A unified VLAN planning is implemented between enterprise branches, and important services and general services are in different VLAN ranges. The enterprise network can use the flexible QinQ based on C-Tag to transparently transmit the internal services of the company, and can also use the service provider network. The QOS policy of the system gives priority to ensuring the data transmission of important services.

As shown in the figure below, the client devices in the metropolitan area network are aggregated through the corridor switches of the community, and broadband Internet access and IPTV services are distinguished by assigning different VLANs to enjoy different QoS service policies.

- In the public network, different service flows of broadband Internet access and IPTV are transmitted in different VLANs to realize transparent transmission of user services.
- □The ISP network sets the QOS policy for the VLAN, and the corresponding VLAN can be encapsulated for the user service on the edge device of the service provider, so that the IPTV service is transmitted preferentially in the ISP network.



Illustration：

- CE1 and CE2 are the edge devices connecting the user network, and PE1 and PE2 are the edge devices of the provider's service network.
- □ On CE1 and CE2, VLAN 1-100 is the user's broadband Internet service flow, and VLAN 101-200 is the user's IPTV service flow.
- □PE1 and PE2 encapsulate different S-Tags for different service VLANs to distinguish different service data. VLAN 1-100 encapsulates VLAN 100, and VLAN 101-200 encapsulates VLAN 200.

PE1 and PE2 are configured exactly the same:

- Configure VLAN

```
SWITCH(config)#vlan 2-200
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#switchport mode hybrid
SWITCH(config-if)#switchport hybrid untagged vlan 100,200
SWITCH(config-if)#switchport hybrid vlan 100
SWITCH(config-if)#interface gigabitEthernet0/2
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#exit
```

- Configure flexible QINQ

```
SWITCH(config)#vlan-vpn isp
SWITCH(config-vlan-vpn)# cvlan 1-100 svlan 100
SWITCH(config-vlan-vpn)# cvlan101-200 svlan 200
SWITCH(config-vlan-vpn)# interface gigabitEthernet0/1
SWITCH(config-if)#switchport vlan-stacking vpn isp
SWITCH(config-if)#exit
```

Case 3: Implementing Layer 2 VPN and Service Flow Management Based on C-Tag VLAN Mapping

Similar to Case 2, the broadband Internet access service and the IPTV service of the user are distinguished. For example, the broadband Internet access service is VLAN2, and the IPTV service is VLAN3. In the ISP network, VLAN200 and VLAN300 are respectively used to represent broadband Internet access services and IPTV services. All ports 1-10 of the PE device are connected to the CE device, and the uplink interface is gigabitEthernet0/11

PE1 and PE2 are configured exactly the same:

- Configure VLAN

```
SWITCH(config)#vlan2-3,200,300
SWITCH(config)#interface gigabitEthernet0/1-10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#exit
```

- Configure VLAN Mapping

```
SWITCH(config)#vlan-vpn isp-map
SWITCH(config-vlan-vpn)#cvlan 2 svlan 200
SWITCH(config-vlan-vpn)#cvlan 3 svlan 300
SWTICH(config-vlan-vpn)#interface gigabitEthernet0/1-10
SWITCH(config-if)#switchport vlan-mapping vpn isp-map
SWITCH(config-if)#exit
```

8.5. DISPLAY COMMAND

- Display the related configuration under the interface

Use show running-configure or show running-configure interfaceIFNAME to display the relevant configuration under the interface.

- Display VPN configuration

In privileged mode, configuration mode, VLAN-VPN mode, and interface mode all support VPN configuration display commands

- **show vlan-vpn***VPN-NAME*: View a certain VPN information.

```
SWITCH#show vlan-vpn test
------------------------------------------------------------
VLAN VPN: test            ==》 VPN name
Class: vlan-stacking      ==》Indicates that the VPN is used for VLAN-
STACKING. If it is not associated with any interface, it is unknown.
```

```
        Mapping attributes:       ==》 The mapping relationship between CVLAN and
SVLAN, if no mapping relationship is configured, it is empty!
         cvlan 1-25,73,75-80 svlan 3
         cvlan 200 svlan 4
        Applied interfaces:       ==》A list of all interfaces associated with
this VPN, or empty if not associated with any interface yet!
         gigabitEthernet0/17
         gigabitEthernet0/18
```

2）show vpn-vpn：View all VPN information.

```
        SWITCH#show vlan-vpn
        ------------------------------------------------------------
        VLAN VPN: test
        Class: vlan-stacking
        Mapping attributes:
         cvlan 1-25,73,75-80 svlan 3
         cvlan 200 svlan 4
        Applied interfaces:
         gigabitEthernet0/17
         gigabitEthernet0/18
        ------------------------------------------------------------
        VLAN VPN: test-map1
        Class: vlan-mapping
        Mapping attributes:
         cvlan 100 svlan 1
         cvlan 200 svlan 2
         cvlan 800 svlan 8
         cvlan 900 svlan 9
        Applied interfaces:
         gigabitEthernet0/18
         gigabitEthernet0/19
        ------------------------------------------------------------
        VLAN VPN: test1
        Class: unkown
        Mapping attributes:
         cvlan 800 svlan 8
         cvlan 900 svlan 9
        Applied interfaces:
         empty!
```

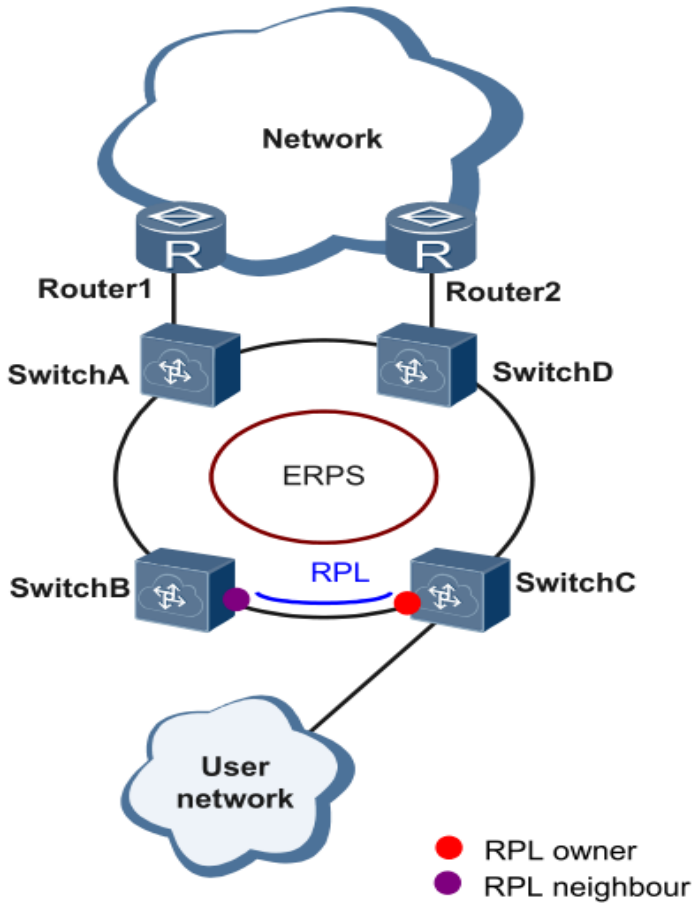
9. CONFIGURE ERPS

9.1. ERPS FUNCTION OVERVIEW

ERPS (Ethernet Ring Protection Switching, Ethernet Ring Protection Switching Protocol) is a ring network protection protocol developed by ITU, also known as G.8032. It is a link layer protocol specially applied to the Ethernet ring network. It can prevent the broadcast storm caused by the data loop when the Ethernet ring network is complete, and can quickly restore the communication between each node on the ring network when a link on the Ethernet ring is disconnected.

At present, the technology to solve the Layer 2 network loop problem is STP. The STP application is relatively mature, but its convergence time is relatively long (second level). ERPS is a link layer protocol specially applied to the Ethernet ring network. The layer 2 convergence performance is within 50ms, and it has a faster convergence speed than STP.

ERPS Typical networking:



9.2. ERPS INTRODUCTION

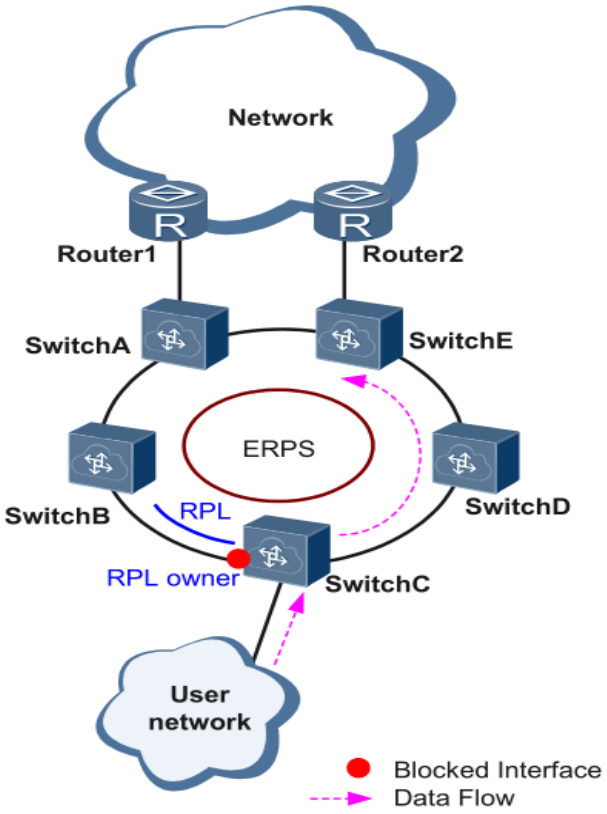
ERPS is a standard ring network protocol dedicated to the Ethernet link layer, with the ERPS ring as the basic unit. Only two ports on each Layer 2 switching device can be added to the same ERPS ring. In an ERPS ring, to prevent a loop from occurring, you can enable the loop-breaking mechanism to block the RPL owner port to eliminate the loop. When a link failure occurs on the ring network, the device running the ERPS protocol can quickly release the blocked port, perform link protection switching, and restore link communication between nodes on the ring network. This section mainly introduces the basic

implementation principle of ERPS in a single-ring network according to the process of link normal -> link failure -> link recovery (including protection switching operation) in the form of an example.

link is normal

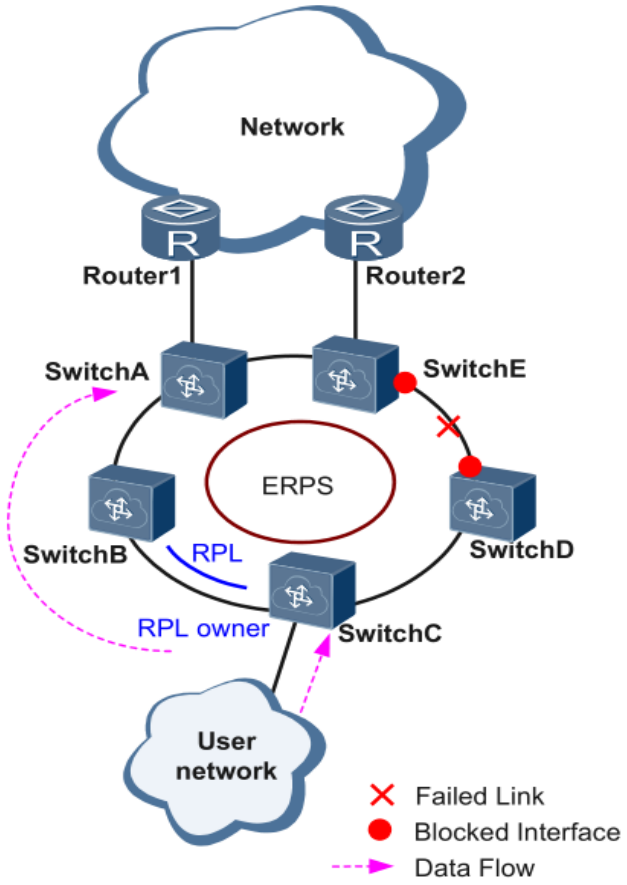
As shown in the following figure, the devices on the ring formed by SwitchA to SwitchE communicate normally.

To prevent loops, ERPS first blocks the RPL owner port. If the RPL neighbor port is configured, the port will also be blocked, and other ports can forward service traffic normally.



link failure

As shown in the figure, when the link between SwitchD and SwitchE fails, the ERPS protocol starts the protection switching mechanism, blocks the ports on both ends of the faulty link, and then releases the RPL owner port, and the two ports resume user traffic. receiving and sending, thus ensuring uninterrupted traffic.



link recovery

After the link returns to normal, if the ERPS ring is configured in failback mode, the device where the RPL owner port resides will block the traffic on the RPL link again, and the faulty link will be used again to transmit user traffic.

9.3. CONFIGURE COMMAND

- Create rings

Command	SWITCH(config)#**erps ring** <1-255> **east-interface** IFNAME **west-interface** IFNAME SWITCH(config)#**no erps ring** <1-255>
Description	create/delete ERPS ring; An ERPS ring consists of a group of interconnected Layer 2 switching devices that are configured with the same control VLAN. It is the basic unit of the ERPS protocol and needs to be configured on each device in the ring. The ring number is the unique identifier of the ERPS ring.

- Create ERPS cases

Command	SWITCH(config)#**erps instance** NAME SWITCH(config)#**no erps instance** NAME
Description	Create/delete an ERPS instance; the instance configuration mode will be entered at the same time of creation. For a Layer 2 device running the ERPS protocol, the VLANs that transmit ERPS protocol packets and data packets must be mapped to the protection instance, so that the ERPS protocol can forward or block these packets according to its blocking principle. Otherwise, VLAN packets may cause broadcast storms in the looped network, resulting in network unavailability.

- Associating ERPS instances and rings

Command	SWITCH(config-erps-inst)#**ring** <1-255>
Description	Configure the correspondence between ERPS instances and rings;

- Configure the ERPS instance level

Command	SWITCH(config-erps-inst)#**level** <0-7>
Description	Configure the ERPS instance level

- Configure the configuration template used by the ERPS instance

Command	SWITCH(config-erps-inst)#**profile** NAME
Description	Configure the ERPS configuration template name;

- Configure the RPL role in the ERPS instance

Command	SWITCH(config-erps-inst)#**rpl-role** NAME
Description	Configure the ERPS instance RPL role; An ERPS ring has only one RPL owner port, which is determined by user configuration. The RPL owner port is blocked from forwarding user traffic to prevent loops in the ERPS ring.

- Configuring the management VLAN for instance protection

Command	SWITCH(config-erps-inst)#**vlan** <2-4094> **raps-channel** SWITCH(config-erps-inst)#**no raps-channel**

Description	Configure/delete the management VLAN/data VLAN of the ERPS instance; Each ERPS ring must be configured with a control VLAN. Different ERPS rings cannot use the same control VLAN ID.

- Configuring the instance-protected VLAN Instance

Command	SWITCH(config-erps-inst)#**id** <0-255>
Description	Configure the VLAN Instance protected by the ERPS instance; The relationship between VLAN and Instance can be configured in MST mode; by default, all VLANs belong to Instance 0; the default id is 0. Note: Multi-instance functionality is currently not supported in intersecting rings!

- Configure the blocking interface of the intersecting sub-ring

Command	SWITCH(config-erps-inst)#**sub-ring block (east-interface | west-interface)**
Description	Configure the ERPS instance as a sub-ring instance and specify the sub-ring to block the interface.

- Configure sub-ring virtual channels and non-virtual channels

Command	SWITCH(config-erps-inst)#**virtual-channel attached-to-instance** NAME SWITCH(config-erps-inst)# **non-virtual-channel**
Description	Configure the type of ERPS intersecting subrings: virtual channel and associated main ring; or non-virtual channel type. Note: The position displayed by this command in showrunning-config must be after the displayed position of the associated instance. Usually, you only need to ensure that the sub-ring ID and instance name are larger than the ID and instance name of the main ring.

- Create ERPS configuration template

Command	SWITCH(config)#**erps profile** NAME

	SWITCH(config)#**no erps profile** NAME
Description	Create/delete ERPS configuration template; enter ERPS template configuration mode after successful creation

- Configure ERPS switchback mode

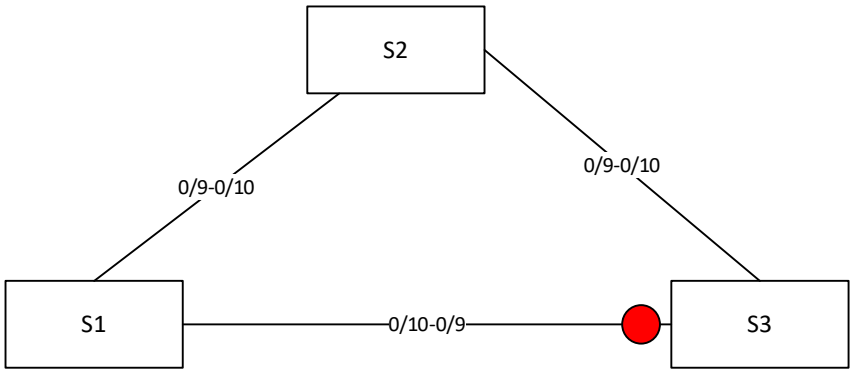
Command	SWITCH(config-erps-prof)#**revertive | non-revertive**
Description	Configure ERPS to automatically switch back/not switch back;

- Configure ERPS timer parameters

Command	SWITCH(config-erps-prof)#**timer** (**wait-to-restore** (<1-12> | **default**) | **hold-off** (<0-100> | **default**) | **guard-timer** (<1-200> | **default**))
Description	Configure ERPS timer parameters; <1-12>: The unit is minute; the switchback time after fault recovery, the default is 5 minutes <0-100>: The unit is 100 milliseconds; the hold time before port forwarding, the default is 0, and direct forwarding is not delayed <1-200>: The unit is 10 milliseconds; the protection window when the state changes, to avoid the misjudgment of the protocol caused by the message of the previous state, the default value is 50: 500 milliseconds The guard-timer parameter will limit the network scale to a certain extent. It is conservatively recommended that when there are more than 300 nodes in the ring network, this parameter should be set to the maximum value, so as to avoid that old packets cannot be discarded normally due to the excessive network scale; 300 No special configuration is required for the internal nodes.

9.4. CONFIGURE CASE

1. Single-ring case requirements: As shown in the figure, the configuration blocks the direct links of S1 and S2 by default, and restores the link in time to ensure the availability of the network in case of failure. Where the data VLANs are 1, 2 and 3.



S1/S2:

- Enter the global configuration mode, create ERPS and set relevant parameters. The command reference list is as follows:

Create data vlan 2,3; vlan 1 exists by default

```
SWITCH(config)#vlan 2,3
```

Change the interface mode to trunk. By default, trunk mode will add all data vlans and management vlans to the interface for forwarding.

```
SWITCH(config)#interface gigabitEthernet0/9-10
SWITCH(config-if)#switchport mode trunk
```

Create erps ring 1

```
SWITCH(config)#erps ring 1 east gigabitEthernet0/9 west
gigabitEthernet0/10
```

Create erps instance 1, associate ring 1, and configure related details

```
SWITCH(config)#erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role non-owner
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

S3:

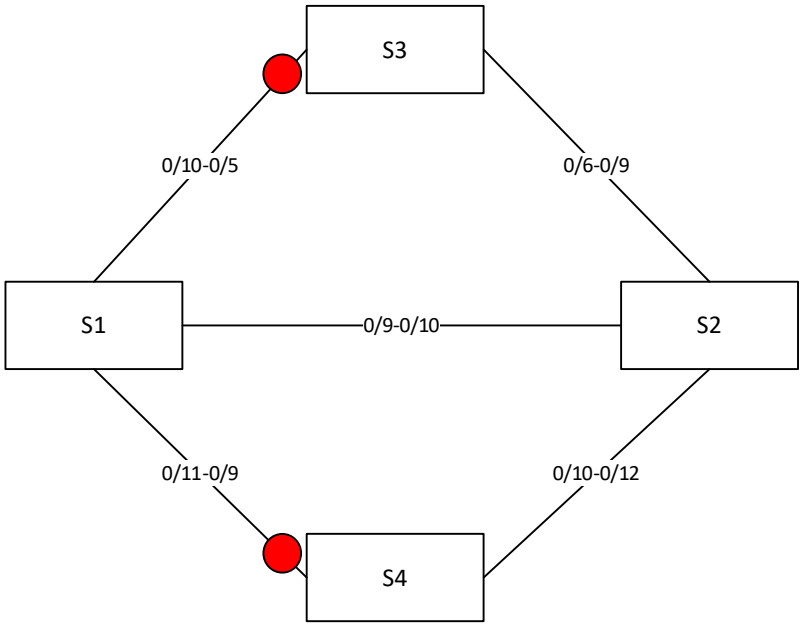
- Enter the global configuration mode, create ERPS and set relevant parameters. The command reference list is as follows:

```
SWITCH(config)#Vlan 2,3
```

```
SWITCH(config)#interface gigabitEthernet0/9,gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#Erps ring 1 east gigabitEthernet0/9 west
gigabitEthernet0/10
SWITCH(config)#Erps instance 1
SWITCH(config-erps-inst)#ring 1
SWITCH(config-erps-inst)#rpl-role owner east
SWITCH(config-erps-inst)#vlan 1000 raps-channel
```

2、Intersecting Ring Case Requirements

As shown in the following topology, S1, S2, S3, and S4 form intersecting rings, and the data vlans are 1, 2, 3, and 4. It is required to achieve fast convergence when a single point of failure occurs in each ring; a maximum of two faults can occur in the network Points (different rings), without user disconnection, to achieve optimal reliability.



Typical configuration example:

S1:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
```

```
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/11
Erps instance 2
 ring 2
  sub-ring block east-interface
  vlan 1100 raps-channel
  virtual-channel attached-to-instance 1
```

S2:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/12 west gigabitEthernet0/10
Erps instance 2
 ring 2
  sub-ring block east-interface
  vlan 1100 raps-channel
  virtual-channel attached-to-instance 1
```

S3:

```
Vlan 2,3,4
interface gigabitEthernet0/5-6
switchport mode trunk
Erps ring 1 east gigabitEthernet0/5 west gigabitEthernet0/6
Erps instance 1
 ring 1
 rpl-role owner east
 vlan 1000 raps-channel
```

S4:

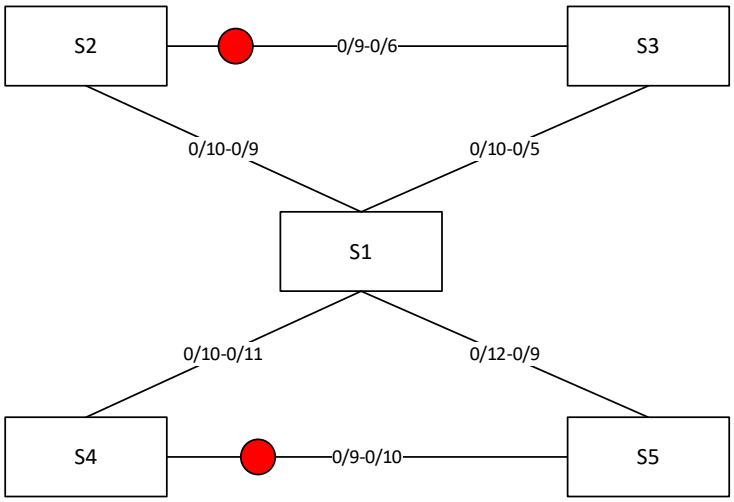
```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 2
```

```
 ring 2
 rpl-role owner east
 vlan 1100 raps-channel
```

3、Tangent Ring Case Requirements

The topology diagram is shown below. S1 is located in the central computer room, which can be supervised and maintained by the administrator in real time, and has high reliability; S2-S5 are distributed in various deployment points, in order to improve the reliability of the network and avoid the occurrence of single-link external connection The single-point failure risk is avoided, and the single-machine failure risk that may occur in a dual-link external connection is avoided, and the dual-link external connection is used to form a ring network.

It is required that each ring network can converge quickly when a single point of failure occurs to avoid user network interruption.



Typical configuration example:

S1:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 vlan 1000 raps-channel

Erps ring 2 east gigabitEthernet0/11 west gigabitEthernet0/12
```

```
Erps instance 2
 ring 2
  vlan 1100 raps-channel
```

S2:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 1 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 1
 ring 1
 rpl-role owner east
 vlan 1000 raps-channel
```

S3:

```
Vlan 2,3,4
interface gigabitEthernet0/5-6
switchport mode trunk
Erps ring 1 east gigabitEthernet0/5 west gigabitEthernet0/6
Erps instance 1
 ring 1
 vlan 1000 raps-channel
```

S4:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 2
 ring 2
 rpl-role owner east
 vlan 1100 raps-channel
```

S5:

```
Vlan 2,3,4
interface gigabitEthernet0/9-12
switchport mode trunk
Erps ring 2 east gigabitEthernet0/9 west gigabitEthernet0/10
Erps instance 2
 ring 2
 vlan 1100 raps-channel
```

9.5. DISPLAY COMMAND

- Display ERPS Ring information

```
SWITCH#show erps ring 1
Ring     : 1
==========
Bridge   : 1
East     : gigabitEthernet0/9
West     : gigabitEthernet0/10
ERP Inst :1,
```

- Display ERPS case

```
SWITCH#
SWITCH#show erps instance 1
Inst Name       : 1
Inst Id         : 0
State           : ERPS_ST_IDLE
Last Priority   : RAPS-NR-RB
Phy Ring        : 1
Role            : NON-OWNER
East Link       : Link_Unblocked(up)(00-D0-FA-0A-10-06, 1)
West Link       : Link_Unblocked(up)(00-D0-FA-0A-10-06, 1)
TCN Propagation : Disabled
Attached        : -
Attached To     : -
Virtual ID      : -:-
-------------------------------------------------------------
    Channel         |       Interface                |  Profile
 (LEVL, VID, RID)   | (east,ver) ,   (west,ver)      |
=============================================================
 (0, 1000,    1)    | (gigabitEthernet0/9, V=1), (gigabitEthernet0/10,
V=1)     | Default
```

- Display ERPS configuration

```
SWITCH#show erps profile 1
Profile : 1
==========
 Wait-To-Restore : 5 mins
 Hold Off Timer  : 0 secs
 Guard Timer     : 500 ms
 Wait-To-Block   : 5500 ms
 Protection Type : Revertive
```

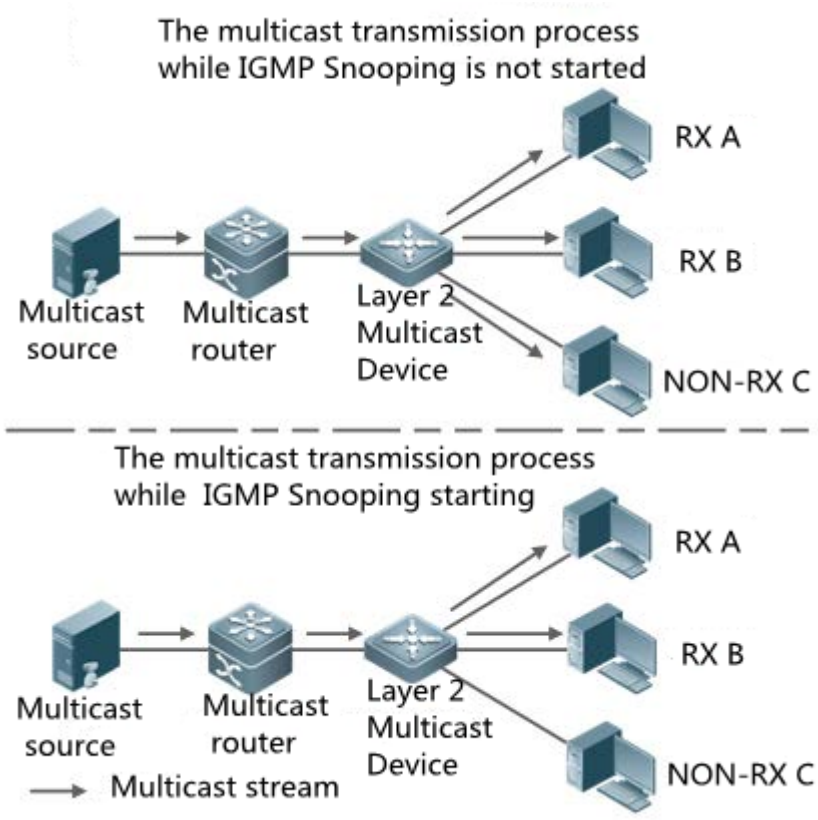
10. CONFIGURE IGMP SNOOPING

10.1. OVERVIEW

IGMP Snooping is the abbreviation of Internet Group Management Protocol Snooping (Internet Group Management Protocol Snooping). It is a multicast-constrained mechanism running on Layer 2 devices to manage and control multicast groups.

A Layer 2 device running IGMP Snooping analyzes the received IGMP packets, establishes a mapping relationship between ports and MAC multicast addresses, and forwards multicast data according to the mapping relationship. When the Layer 2 device does not run IGMP Snooping, the multicast data is broadcast at Layer 2; when the Layer 2 device runs IGMP Snooping, the multicast data of the known multicast group will not be broadcast at Layer 2, but at Layer 2. is multicast to the specified receivers.

As shown in the figure below, when the Layer 2 multicast device does not run IGMP Snooping, the IP multicast packets are broadcast in the VLAN; when the Layer 2 multicast device runs IGMP Snooping, the IP multicast packets are only sent to the group members recipient.



10.2. CONFIGURE COMMAND

- Start IGMP Snooping

Command	SWITCH(config)#**igmp snooping** SWITCH(config)#**no igmp snooping**
Description	Enable/disable the IGMP Snooping function; disabled by default. Global mode.

- Configure IGMP Snooping uplink

Command	SWITCH(config-if)#**igmp snooping mrouter interface** IFNAME SWITCH(config-if)#**no igmp snooping mrouter interface** IFNAME
Description	Create /delete IGMP Snooping Uplink； optional configuration. SVI interface mode.

- Configure IGMP Snooping static group

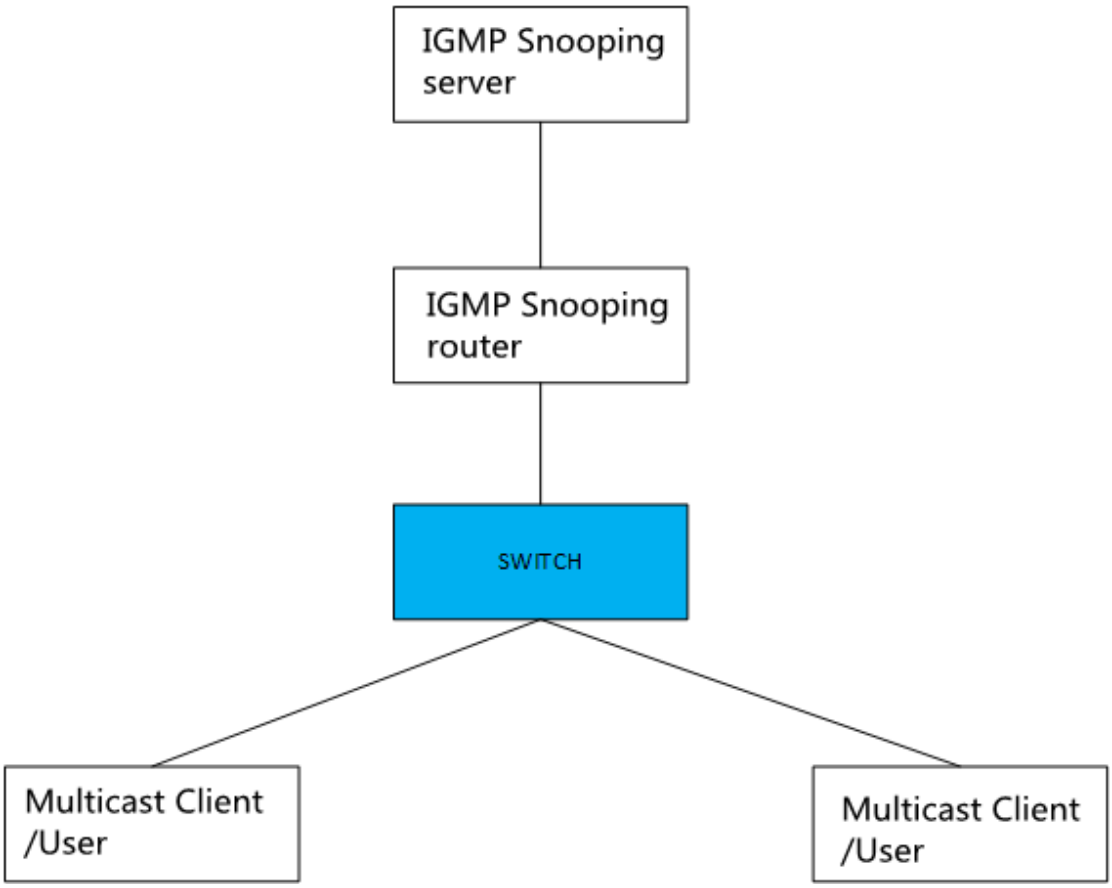
Command	SWITCH(config-if)#**igmp snooping static-group** IPADDR **source** IPADDR **interface** IFNAME SWITCH(config-if)#**no igmp snooping static-group** IPADDR **source** IPADDR **interface** IFNAME
Description	Configure /delete IGMP Snooping static group； optional configuration. SVI interface mode.

- Configure IGMP Snooping to leave fast

Command	SWITCH(config-if)#**igmp snooping fast-leave** SWITCH(config-if)#**no igmp snooping fast-leave**
Description	configure/delete IGMP Snooping fast-leave function;optional configuration. SVI interface mode.

10.3. CONFIGURE CASE

Simplified topology:



Basic configuration/roles: (top-down)

server:

The multicast service needs to be enabled. During the test, VLC is used as the multicast server to provide the multicast service: udp://225.0.0.1:1234, the server IP is 3.3.3.10

router:

Run the multicast routing protocol and enable IGMP, and use Ruijie S57 Layer 3 switch to simulate the test. The main configurations are as follows:

Enable multicast routing

```
ip multicast-routing
```

Configure the uplink port and connect to the server. Here, the PIM dense mode is simply selected. The actual network scale is large and the multicast usage is small. It is recommended to use the sparse mode.

```
interface GigabitEthernet 0/23
 no switchport
 no ip proxy-arp
 ip pim dense-mode
ip address 3.3.3.3 255.255.255.0
```

Configure the downlink port. Here is a simple selection of PIM dense mode. The actual network scale is large and the multicast usage is small. It is recommended to use sparse mode.

```
interface VLAN 1
 no ip proxy-arp
 ip pim dense-mode
ip address 2.2.2.1 255.255.255.0
```

SWITCH:

Multicast can be enabled

```
igmp snooping
```

Client:

Watch server multicast video through udp://225.0.0.1:1234, IP 2.2.2.10

10.4. DISPLAY COMMAND

- View IGMP Snooping Multicast group

```
SWITCH#show igmp snooping groups
```

- View IGMP Snooping interface information

```
SWITCH#show igmp snooping interface {ifname}
eg:
IGMP Snooping information for vlan1
 IGMP Snooping enabled
 Snooping Querier none
 IGMP Snooping other querier timeout is 255 seconds
 Group Membership interval is 260 seconds
 IGMPv2 fast-leave is disabled
 IGMPv1/v2 Report suppression enabled
```

```
 IGMPv3 Report suppression enabled
 Router port detection using IGMP Queries
 Number of router-ports: 2
 Number of Groups: 2
 Number of Joins: 891
 Number of Leaves: 4
 Active Ports:
  gigabitEthernet0/1
  gigabitEthernet0/2
```

- View IGMP Snooping router port information

```
SWITCH#show igmp snooping mrouter vlan1
eg:
SWITCH#show igmp snooping mrouter vlan1
VLAN    Interface             IP-address    Expires
1       gigabitEthernet0/18(dynamic)         2.2.2.1        00:03:34
       gigabitEthernet0/20(static)           --             --
```

- View IGMP Snooping ports statistics

```
SWITCH#show igmp snooping statistics interface vlan1
IGMP Snooping statistics for vlan1
 Group Count            :  2
 IGMP reports received  :  893
 IGMP leaves received   :  4
 IGMPv1 query warnings  :  0
 IGMPv2 query warnings  :  456
 IGMPv3 query warnings  :  0
```

11. CONFIGURE STP PROTOCOL

11.1. OVERVIEW

Spanning Tree Protocol is a Layer 2 management protocol, which eliminates Layer 2 loops by selectively blocking redundant links in the network, and also has the function of link backup.

Like the development process of many protocols, the Spanning Tree Protocol is constantly updated with the development of the network, from the original STP (Spanning Tree Protocol, Spanning Tree Protocol) to RSTP (Rapid Spanning Tree Protocol, Rapid Spanning Tree Protocol), and then To the latest MSTP (Multiple SpanningTree Protocol, Multiple Spanning Tree Protocol).

For Layer 2 Ethernet, there can only be one active path between two LANs, otherwise a broadcast storm will occur. However, in order to strengthen the reliability of a local area network, it is necessary to establish redundant links, some of which must be in a backup state. If the network fails and another link fails, the redundant link must be upgraded to Active status. Controlling such a process manually is obviously a very hard job, and the STP protocol does this automatically. It enables devices on a local area network to:

Find and start an optimal tree topology for the LAN.

Faults are detected and then recovered, automatically updating the network topology so that the best possible tree structure is selected at any time.

11.2. CONFIGURE COMMAND

- Configure STP Mode

Command	SWITCH(config)#**spanning-tree mode** {**stp | rstp | mstp**}
Description	stp：Spanning tree protocol(IEEE 802.1d) rstp：Rapid spanning tree protocol(IEEE 802.1w) mstp：Multiple spanning tree protocol(IEEE 802.1s) The default is rstp mode. After the mode is switched, the spanning tree protocol is disabled by default and needs to be re-enabled. Global mode.

- Start STP protocol

Command	SWITCH(config)#**spanning-tree enable** SWITCH(config)#**no spanning-tree enable**
Description	Enables/disables the STP function; disabled by default.

	Global mode.

- Configure device priority

Command	SWITCH(config)#**spanning-tree priority** <0-61440> SWITCH(config)#**no spanning-tree priority** SWITCH(config)#**spanning-tree instance** <1-63> **priority** <0-61440> SWITCH(config)**#no spanning-tree instance** <1-63> **priority**
Description	Configure/delete STP system priority; default 32768. Optional. Global mode.

- Configure Hello Time

Command	SWITCH(config)#**spanning-tree hello-time** <1-10> SWITCH(config)#**no spanning-tree hello-time**
Description	Configure/reset the BPDU packet period, in seconds; the default is 2s. Optional. Global mode.

- Configure Forward-Delay Time

Command	SWITCH(config)#**spanning-tree forward-time** <4-30> SWITCH(config)#**no spanning-tree forward-time**
Description	Configure/reset the STP port forwarding state delay time, in seconds; the default is 15s. Optional. Global mode.

- Configure Max-Age Time

Command	SWITCH(config)#**spanning-tree max-age** <6-40> SWITCH(config)#**no spanning-tree max-age**

Description	Configure/reset the lifetime of BPDUs, in seconds; the default is 20s. Optional. Hello Time, Forward-Delay Time, Max-Age Time need to follow the conditions: 2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0seconds), otherwise it may lead to topology unstable. The longest path of the STP/RSTP network is affected by this parameter. The default longest path is 20 devices. When there are more than 20 devices, the configuration needs to be modified (forward-delay 21s, max-age 40s can be configured), and the maximum supported longest path is 40 tower. Global mode.

- Configure Max-Hops

Command	SWITCH(config)#**spanning-tree max-hops** <1-40> SWITCH(config)#**no spanning-tree max-hops**
Description	Configure/reset the maximum number of hops for BPDU packets; the default is 20. Optional. The longest path of the MSTP network is affected by this parameter. When there are more than 20 devices, the configuration needs to be modified, with a maximum of 40. MSTP is compatible with the max-age function, and the max-age parameter needs to be adjusted at the same time. Refer to the corresponding command. Global mode.

- Configure Transmit-Holdcount

Command	SWITCH(config)#**spanning-tree transmit-holdcount** <1-10> SWITCH(config)#**no spanning-tree transmit-holdcount**
Description	Configure/reset the maximum number of BPDUs sent per second; default is 6. Optional. Global mode

- Enter MST Mode

Command	SWITCH(config)#**spanning-tree mst configuration**

Description	Enter MST Mode Global Mode

- Configure the corresponding relationship between MST VLAN and instance

Command	SWITCH(config-mst)# **instance** <1-63> **vlan** VLANID SWITCH(config-mst)# **no instance** <1-63> **vlan** VLANID
Description	Configure/delete the association between MST instances and VLANs; optional configuration. MST mode.

- Configure the MST area name

Command	SWITCH(config-mst)#**region** NAME SWITCH(config-mst)#**no region** NAME
Description	Configure/delete the MST area name; optional configuration. MST mode.

- Configure the MST version number

Command	SWITCH(config-mst)#**revision** <0-65535>
Description	Configure/delete the MST version number, the default is 0; optional configuration. MST mode.

- Configure the association between ports and instances

Command	SWITCH(config-if)# **spanning-tree instance** <1-63> SWITCH(config-if)# **no spanning-tree instance** <1-63>
Description	Configure/remove association of ports and instances; optional configuration. By default, when configuring the relationship between an instance and a VLAN, the system automatically generates the relationship data between the port and the

	instance based on the VLAN and port relationship, and no manual configuration is required. After the instance is configured, if the relationship between ports and VLANs is manually modified, such as adding/exiting all VLANs of an instance to the ports, you need to manually maintain the relationship between ports and instances through this command. When major configuration changes occur, it is recommended to automatically generate port and instance data by reconfiguring the instance-VLAN relationship or restarting the device. MST mode.

- Configure port priority

Command	SWITCH(config-if)#**spanning-tree priority** <0-240> SWITCH(config-if)#**spanning-tree instance** <1-63> **priority** <0-240>
Description	Configure the port STP priority; the default is 128. Optional. Interface configuration mode.

- Configure port path cost

Command	SWITCH(config-if)#**spanning-tree path-cost** <1-200000000> SWITCH(config-if)#**no spanning-tree path-cost**
Description	Path cost to configure/reset port; optional configuration. Interface configuration mode.

- Configure Link-Type

Command	SWITCH(config-if)#**spanning-tree link-type** {**auto	point-to-point	shared**} SWITCH(config-if)#**no spanning-tree link-type**
Description	Configure/reset the link type, the default is auto. Optional. auto: Automatic setting mode based on the duplex capability of link negotiation, full duplex is a point-to-point connection.

	point-to-point: Enable fast forwarding. shared: Disable fast forwarding. Global mode.

- Configure Protocol Migration processing

Command	SWITCH(config-if)#**clear spanning-tree detected protocols**
Description	Force version checking on all ports. Privileged mode.

- Turn on Portfast

Command	SWITCH(config-if)#**spanning-tree portfast** SWITCH(config-if)#**no spanning-tree portfast**
Description	Configure/delete port portfast; the port will be forwarded directly after portfast is enabled. However, the Port Fast Operational State will be disabled due to the receipt of BPDUs, so that it can normally participate in the STP algorithm and forwarding; it is disabled by default; optional configuration. Interface configuration mode.

- Configure Edge Port

Command	SWITCH(config-if)#**spanning-tree {edgeport | autoedge}** SWITCH(config-if)#**no spanning-tree {edgeport | autoedge}**
Description	Configure/delete a port Edge Port; if configured as edgeport, it means that the device directly connected to the port is not a bridge device and can be forwarded quickly; if configured as autoedge, it means that the port automatically identifies whether it is an edge port according to the BPDU; it is disabled by default; optional configuration. Interface configuration mode.

- Configure Root Guard

Command	SWITCH(config-if)# **spanning-tree guard root**

	SWITCH(config-if)#**no spanning-tree guard root**
Description	Configure/delete port root guard; when the root guard function is enabled on an interface, its port role on all instances is forced to be the designated port. Once the port receives configuration information with a higher priority, the root guard function will set the interface to the designated port. blocked state; closed by default; optional configuration. Interface configuration mode.

- Configure BPDU Guard

Command	SWITCH(config)#**spanning-tree portfast bpdu-guard** SWITCH(config)#**no spanning-tree portfast bpdu-guard** SWITCH(config-if)#**spanning-tree portfast** SWITCH(config-if)#**no spanning-tree portfast** Or ： SWITCH(config-if)#**spanning-tree bpdu-guard enable** SWITCH(config-if)#**spanning-tree bpdu-guard disable**
Description	Configure/delete BPDU Guard; after the port has BPDU Guard enabled, if a BPDU is received on the port, it will enter the Error-disabled (blocked) state; optional configuration. Interface configuration mode.

- Configure BPDU Filter

Command	SWITCH(config)#**spanning-tree portfast bpdu-filter** SWITCH(config)#**no spanning-tree portfast bpdu-filter** SWITCH(config-if)#**spanning-tree portfast** SWITCH(config-if)#**no spanning-tree portfast** Or ： SWITCH(config-if)#**spanning-tree bpdu-filter enable** SWITCH(config-if)#**spanning-tree bpdu-filter disable**

Description	Configure/delete BPDU Filter; after enabling BPDU Filter, the port neither sends BPDU nor receives BPDU packets; optional configuration. Interface configuration mode.

- Configure TC topology change notification

Command	SWITCH(config-if)#**spanning-tree restricted-tcn** SWITCH(config-if)#**no spanning-tree restricted-tcn** SWITCH(config-if)#**spanning-tree instance** <1-63> **restricted-tcn** SWITCH(config-if)#**no spanning-tree instance** <1-63> **restricted-tcn**
Description	Configure/reset the topology change notification limit. After configuration, the port will not forward TC BPDUs, nor refresh the address table; optional configuration. Interface configuration mode.

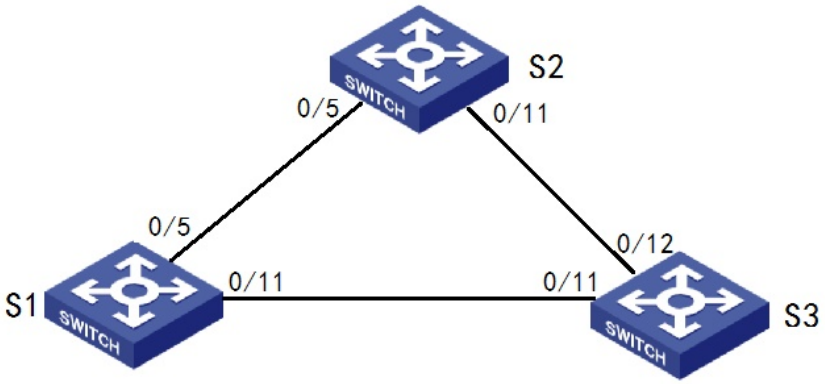
- Configure the wrong port timeout function

Command	SWITCH(config)#**spanning-tree errdisable-timeout enable** SWITCH(config)#**no spanning-tree errdisable-timeout enable** SWITCH(config)#**spanning-tree errdisable-timeout interval** <10-1000000> SWITCH(config)#**no spanning-tree errdisable-timeout interval**
Description	Configure/reset error port timeout feature. By default, the error port timeout function is not enabled, that is, the error port will never timeout and automatically recover, and must be recovered manually. The timeout unit is seconds, the default is 300 seconds; Optional. Global configuration mode.

11.3. CONFIGURE CASE

1、RSTP anti-loop realizes link redundancy scheme

Simplified topology:



Typical configuration：

S1/S2/S3：

- Enter the global configuration mode, configure the rstp mode, and enable the stp switch:

Use rstp Mode

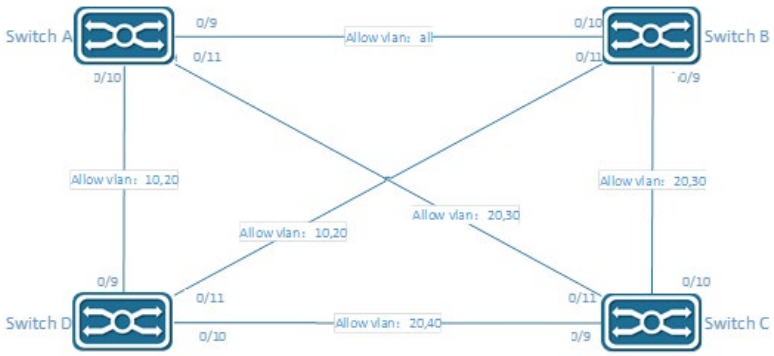
```
spanning-tree mode rstp
```

Enable stp switch

```
spanning-tree enable
```

2、MSTP implements domain- and instance-based anti-loop and link redundancy

Simplified topology:



Configuration plan：

The devices belong to the same domain, the default Default domain is used here, no additional configuration is required

VLAN 20 is a shared vlan and is directly assigned to CST

Case	VLAN
0	20
1	10
3	30
4	40

Typical configuration:

Switch A:

configure VLAN and interface

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
SWITCH(config)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
```

configure MSTP case

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

start MSTP

```
SWITCH(config)#spanning-tree enable
```

Switch B:

configure VLAN and interface

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
```

configure MSTP case

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

start MSTP

```
SWITCH(config)#spanning-tree enable
```

Switch C:

configure VLAN and interface

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,40
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
SWITCH(config)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,30
```

configure MSTP case

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

start MSTP

```
SWITCH(config)#spanning-tree enable
```

Switch D:

configure VLAN and interface

```
SWITCH(config)#vlan 10,20,30,40
SWITCH(config)#interface gigabitEthernet0/9
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 20,40
SWITCH(config)#interface gigabitEthernet0/11
SWITCH(config-if)#switchport mode trunk
SWITCH(config-if)#switchport trunk allowed vlan 10,20
```

configure MSTP case

```
SWITCH(config)#spanning-tree mode mstp
SWITCH(config)#spanning-tree mst configuration
SWITCH(config-mst)#instance 1 vlan 10
SWITCH(config-mst)#instance 3 vlan 30
SWITCH(config-mst)#instance 4 vlan 40
```

Start MSTP

```
SWITCH(config)#spanning-tree enable
```

11.4. DISPLAY COMMAND

- View STP state

```
SWITCH#show spanning-tree
```

- View MSTP case state

```
SWITCH#show spanning-tree mst instance <1-63>
```

12. MAC ADD MANAGEMENT

12.1. MAC ADD OVERVIEW

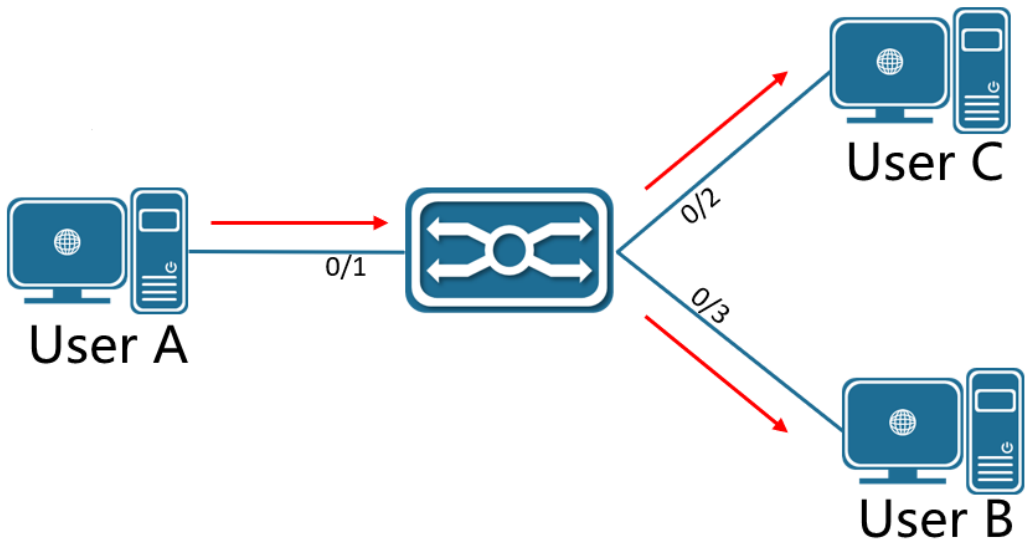
The Ethernet switch parses the destination MAC address carried in the packet, queries the MAC address table, and sends the packet to the corresponding port. The MAC address table records the MAC address, interface and VLAN ID information of the device connected to the device. The Ethernet switch decides to use the well-known unicast or unknown-name broadcast forwarding mode according to the result of the MAC address table lookup.

Well-known unicast: The Ethernet switch finds the entry corresponding to the destination MAC address and VLAN ID of the packet in the MAC address table, and the output port in the entry is unique, and the packet is output directly from the port corresponding to the entry .

Unknown name broadcast: The Ethernet switch does not find the entry corresponding to the target MAC address in the address table, and the packet is sent to all other ports in the VLAN to which it belongs except the packet input port for output.

The MAC address of the Ethernet switch can be obtained dynamically or statically. Generally, it is obtained dynamically. The working principle of dynamic MAC address learning is given below by analyzing the interaction process between user A and user C.

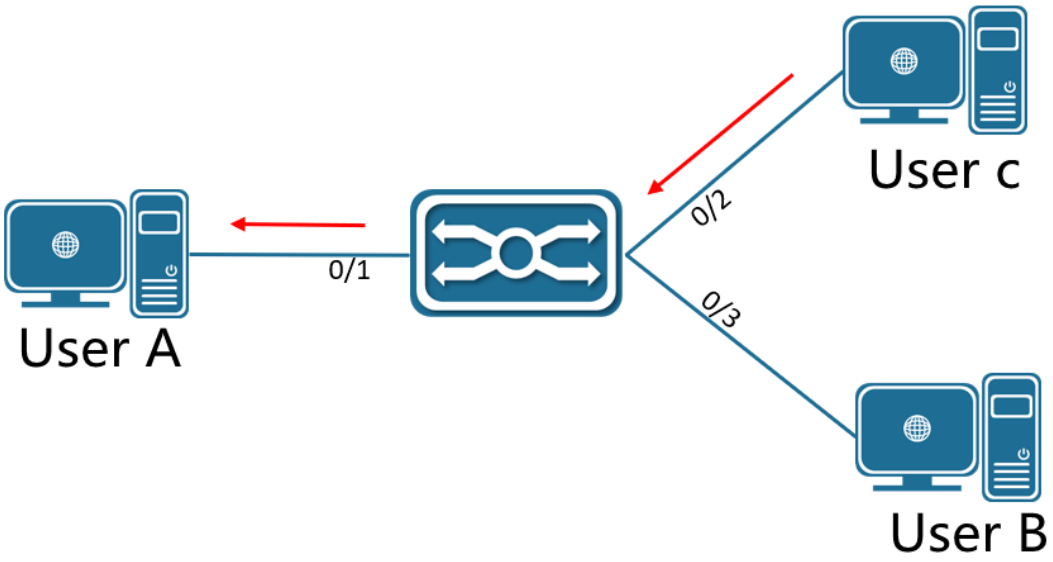
User A sends a packet to port gigabitEthernet0/1 of the switch. At this time, the Ethernet switch learns the MAC address of user A into the MAC address table. Since there is no source MAC address of user C in the address table, the Ethernet switch broadcasts the packet to all ports in VLAN1 except gigabitEthernet0/1 connected to user A, including the ports of user B and user C. At this time, user B can receive the packets sent by user A that do not belong to it.



Current dynamic MAC address table information:

USER	VLAN	MAC address	Port
User A	1	000E.C6C1.C8AB	gigabitEthernet0/1

After receiving the packet, user B sends the response packet to user A through port gigabitEthernet0/2 of the Ethernet switch. At this time, the MAC address of user A already exists in the MAC address table of the Ethernet switch, and the packet is unicast. It is forwarded to the gigabitEthernet0/1 port, and the Ethernet switch will learn the MAC address of user C. The difference from the previous one is that user B cannot receive the packets sent by user C to user A at this time.



Current dynamic MAC address table information:

User	VLAN	MAC Address	PORT
User A	1	000E.C6C1.C8AB	gigabitEthernet0/1
User C	1	000E.C6C1.C8AD	gigabitEthernet0/2

After an interaction between user A and user C, the device learns the source MAC addresses of user A and user C, and then the packet interaction between user A and user C is forwarded by unicast. The interaction packets between user A and user C are no longer received.

12.2. CONFIGURE COMMAND

- Configuring the Dynamic MAC Address Aging Time

Command	SWITCH(config)#**mac-address-table aging-time** <0-600> SWITCH(config)#**no mac-address-table aging-time**
Description	Configure the MAC address aging time, the range is 0-600 seconds; The default MAC address aging time is 300 seconds; When set to 0, it means to disable the MAC address aging function;

- Configure a static MAC address

Command	SWITCH(config)#**mac-address-table static** MAC_ADDR **vlan** VLANID **interface** IFNAME SWITCH(config)#**no mac-address-table static** MAC_ADDR **vlan** VLANID **interface** IFNAME
Description	Configure a static MAC address; When the device receives a packet with MAC_ADDR as the destination address on the VLAN specified by VLANID, the packet will be forwarded to the interface specified by IFNAME; IFNAME supports physical ports and aggregate ports

- Configuring MAC Address Filtering

Command	SWITCH(config)#**mac-address-table filter** MAC_ADDR **vlan** VLANID SWITCH(config)#**no mac-address-table filter** MAC_ADDR **vlan** VLANID
Description	Configure MAC address filtering; When the device receives a packet with the address specified by MAC_ADDR as the source or destination address on the VLAN specified by VLANID, it will be discarded.

- Clear dynamic MAC address

Command	SWITCH#**clear mac-address-table dynamic** SWITCH#**clear mac-address-table dynamic vlan** VLANID SWITCH#**clear mac-address-table dynamic interface** IFNAME
Description	Dynamic MAC address clearing operation; Supports all, VLAN-based, and port-based MAC address clearing operations

12.3. CONFIGURE CASE

Case 1: Configure the dynamic MAC address aging time to 60 seconds.

- Enter global mode ：

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

- Configuring Dynamic Address Aging Time

```
SWITCH(config)#mac-address-table aging-time 60
```

Case 2: Configure a static MAC address, all destination MAC addresses are 000E.C6C1.C8AB, and packets of VLAN 1 are forwarded from port gigabitEthernet0/1.

- Enter global mode :

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

- Configure a static MAC address

```
SWITCH(config)#mac-address-table static 000E.C6C1.C8AB vlan 1 interface
gigabitEthernet0/1
```

Case 3: Configure MAC address filtering to discard packets whose source or destination MAC address is 000E.C6C1.C8AB in VLAN 1.

- Enter global mode：

```
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

- To configure filtering by MAC address:

```
SWITCH(config)#mac-address-table filter 000E.C6C1.C8AB vlan 1
```

Case 4: Clear the dynamic MAC address under port gigabitEthernet0/1.

- Clear dynamic MAC address

```
SWITCH#clear mac-address-table dynamic interface gigabitEthernet0/1
```

12.4. DISPLAY COMMAND

- Display MAC address

```
SWITCH#show  mac-address-table
 VLAN     MAC Address     Type      Ports
  -----+---------------+---------+----------------------+
  20     0000.0000.0009   filter    drop
  20     0000.0000.000a   filter    drop
```

- Display MAC address statistics

```
SWITCH#show  mac-address-table count
Static Address Count: 0
Filter Address Count: 2
Dynamic Address Count: 0
```

13. CONFIGURE LLDP

1.1. PROTOCOL OVERVIEW

LLDP (Link Layer Discovery Protocol, Link Layer Discovery Protocol) provides a standard link layer discovery method, enabling devices of different manufacturers to discover each other in the network and exchange their system and configuration information. LLDP encapsulates the information of the local device (including main capabilities, management addresses, device identification, interface identification, etc.) in LLDPDU (Link Layer Discovery Protocol Data Unit, link layer discovery protocol data unit) and publishes it to its directly connected neighbors , the neighbors will save the information in the form of standard MIB after receiving the information, so that the network management system can query and judge the communication status of the link.

LLDPDU

LLDPDU is a data unit encapsulated in the data part of an LLDP message. Before forming an LLDPDU, the device first encapsulates the local information into a TLV format, and then combines several TLVs into one LLDPDU and encapsulates it in the data part of the LLDP packet for transmission.

Figure 22 -1 Encapsulation format of LLDPDU



As shown in Figure 22-1, the blue Chassis ID TLV, Port ID TLV, and Time To Live TLV are mandatory for each LLDPDU, and the rest of the TLVs are optional. Each LLDPDU can carry up to 32 TLVs.

TLV

TLV is the unit that makes up LLDPDU, and each TLV represents a piece of information. The TLVs that LLDP can encapsulate include basic TLVs, 802.1 organization-defined TLVs, 802.3 organization-defined TLVs, and LLDP-MED (Link Layer Discovery Protocol Media Endpoint Discovery, Link Layer Discovery Protocol Media Endpoint Discovery) TLVs.

Basic TLV

Basic TLVs are a set of TLVs that are the basis for network device management. 802.1 organization-defined TLVs, 802.3 organization-defined TLVs, and LLDP-MED TLVs are TLVs defined by standards organizations or other organizations to enhance the management of network devices. Need to choose whether to send in LLDPDU.

Among the basic TLVs, there are several TLVs that are mandatory to implement the LLDP function, that is, they must be published in the LLDPDU, as shown in Table 22 -1.

Diagram. 22-1 basic TLV

TLV Name	Illustration	Is it mandatory to publish
Chassis ID	Bridge MAC address of the sending device	yes
Port ID	Identifies the port of the sender of the LLDPDU. If LLDP-MED TLV is carried in LLDPDU, its content is the MAC address of the port; otherwise, its content i s the name of the port	yes
Time To Live	The survival time of this device information on the n eighbor device	Yes
End of LLDPDU	The end identifier of the LLDPDU, which is the last TLV of the LLDPDU	No
Port Description	Port Description	No
System Name	Device Name	No
System Description	System Description	No
System Capabilities	The main functions of the system and the function it ems that have been turned on	No
Management Address	Management address, as well as the interface numb er and OID (Object Identifier) corresponding to the address	No

802.1Organization-Defined TLV

The content of TLV defined by IEEE 802.1 organization is shown in Table 22- 2.

Currently, H3C devices do not support sending Protocol Identity TLV and VID Usage Digest TLV, but can receive these two types of TLVs.

Layer 3 Ethernet interfaces only support Link Aggregation TLVs.

Diagram 22-2 IEEE 802.1 ***Organization-Defined TLV***

TLV Name	Illustration
Port VLAN ID(PVID)	Port VLAN ID
Port and protocol VLA N ID(PPVID)	Port protocol VLAN ID

TLV Name	Illustration
VLAN Name	The name of the VLAN to which the port belongs
Protocol Identity	The type of protocol supported by the port
DCBX	Data Center Bridging Exchange Protocol
EVB Module	(Not currently supported) Edge Virtual Bridging module, including EV B TLV and CDCP (S-Channel Discovery and Configuration Protocol, S-Channel Discovery and Configuration Protocol) TLV. For the detail ed introduction of these two TLVs, please refer to "EVB Configuratio n Guide"
Link Aggregation	Whether the port supports link aggregation and whether link aggreg ation is enabled
Management VID	Manage VLAN
VID Usage Digest	Data containing a summary of VLAN ID usage
ETS Configuration	Enhanced Transmission Selection configuration
ETS Recommendation	Enhanced transfer selection recommendation
PFC	Priority-based Flow Control
APP	Application Protocol
QCN	(Not currently supported) Quantized Congestion Notification

802.3Organization-Defined TLV

The content of TLV defined by IEEE 802.3 organization is shown in Table 22-3.

The Power Stateful Control TLV was defined in the IEEE P802.3at D1.0 version, and later versions no longer support this TLV. The H3C device will only send this type of TLV after receiving the Power Stateful Control TLV.

*Diagram 22-3 IEEE 802.3**Organization-Defined TLV***

TLV Name	Illustration
MAC/PHY Configuration/Sta tus	The rate and duplex status supported by the port, whether it supports port rate auto-negotiation, whether the auto-negotiation function is enabled, and the current rate and duplex status
Link Aggregation	Whether the port supports link aggregation and whether link aggregation is enabled

TLV Name	Illustration
Power Via MDI	The power supply capability of the port, including the type of PoE (Power over Ethernet, Power over Ethernet) (including PSE (Power Sourcing Equipment, Power Sourcing Equipment) and PD (Powered Device, Powered Device)), the remote power supply mode of the PoE port, Whether PSE power supply is supported, whether PSE power supply is enabled, whether the power supply mode is controllable, power supply type, power source, power priority, PD request power value, and PSE power distribution value
Maximum Frame Size	Maximum frame length supported by the port
Power Stateful Control	Power status control of ports, including the type of power used by the PSE/PD, the priority of supplying/receiving power, and the power supplied/received
Energy-Efficient Ethernet	Energy Efficient Ethernet

Manage address

The management address is an address for the network management system to identify and manage network devices. The management address can clearly identify a device, which facilitates the drawing of network topology and facilitates network management. The management address is encapsulated in the Management Address TLV of the LLDP packet and advertised.

Working Mode of LLDP

Under the specified type of LLDP proxy, LLDP has the following four working modes:

- □TxRx: Both send and receive LLDP packets.
- □Tx: Only send but not receive LLDP packets.
- □Rx: Only receive and do not send LLDP packets.
- □Disable: neither send nor receive LLDP packets.

When the LLDP working mode of the port changes, the port will initialize the protocol state machine. To prevent the port from continuously performing initialization operations due to frequent changes in the working mode of the port, you can configure the port initialization delay time.

Protocol Specification

The protocol specifications related to LLDP are:

- IEEE 802.1AB-2005：Station and Media Access Control Connectivity Discovery

- IEEE 802.1AB 2009：Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057：Link Layer Discovery Protocol for Media Endpoint Devices
- IEEE Std 802.1Qaz-2011：Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes

1.2. CONFIGURE COMMAND

1.2.1. Switch and working mode configuration

- Globally enable/disable the LLDP function

Command	SWITCH(config)# **lldp run** SWITCH(config)#**no lldp run**
Description	Global configuration mode. Enable/disable LLDP function. required.

- Enter LLDP interface proxy configuration mode

Command	SWITCH(config-if)# **lldp-agent** SWITCH(lldp-agent)# **exit**
Description	Interface configuration mode. Enter the LLDP interface proxy configuration mode. Optional.

- Configure the working mode of the LLDP interface

Command	SWITCH(lldp-agent)# **lldp enable** { rxonly | txonly | txrx } SWITCH(lldp-agent)# **lldp disable**
Description	LLDP interface proxy configuration mode. Configure the working mode of the LLDP interface. Optional.

1.2.1. Optional basic parameter configuration

- Configure the system name

Command	SWITCH(config)# **lldp system-name** NAME SWITCH(config)# **no lldp system-name**
Description	Global configuration mode. Configure/reset the system name. Optional.

- Configuration system descriptor

Command	SWITCH(config)# **lldp system-description** LINE SWITCH(config)# **no lldp system-description**
Description	Global configuration mode. Configure/reset system descriptors. Optional.

- Configure device locally-assigned

Command	SWITCH(config)# **lldp chassis locally-assigned** NAME SWITCH(config)# **no lldp chassis locally-assigned**
Description	Global configuration mode. Configure/reset the device locally-assigned. Optional.

- Configure Port locally-assigned

Command	SWITCH(config-if)# **lldp locally-assigned** NAME SWITCH(config-if)# **no lldp locally-assigned**
Description	Interface configuration mode. Configure/reset the interface locally-assigned. Optional.

- Configuring the interface proxy cable ID

Command	SWITCH(config-if)# **lldp agt-circuit-id** VALUE SWITCH(config-if)# **no lldp agt-circuit-id**

Description	Interface configuration mode. Configure/reset interface agt-circuit-id. Optional.

- Configure the interface port descriptor

Command	SWITCH(config-if)# **lldp port-description** LINE SWITCH(config-if)# **no lldp port-description**
Description	Interface configuration mode. Configure/reset interface port descriptors. Optional.

- Configure the device ID type of the LLDP interface

Command	SWITCH(lldp-agent)# **lldp chassis-id-tlv** { if-alias | if-name | ip-address | locally-assigned | mac-address } SWITCH(lldp-agent)# **no lldp chassis-id-tlv**
Description	LLDP interface proxy configuration mode. Configure the device identification type of the LLDP interface. Optional.

- Configure the management address type of the LLDP interface

Command	SWITCH(lldp-agent)# **lldp management-address-tlv** { ip-address | mac-address } SWITCH(lldp-agent)# **no lldp management-address-tlv**
Description	LLDP interface proxy configuration mode. Configure the management address type of the LLDP interface. Optional.

- Configure the port ID type of the LLDP interface

Command	SWITCH(lldp-agent)# **lldp port-id-tlv** { agt-circuit-id | if-alias | if-name | ip-address | locally-assigned | mac-address }

	SWITCH(lldp-agent)# **no lldp port-id-tlv**
Description	LLDP interface proxy configuration mode. Configure the port ID type of the LLDP interface. Optional.

1.2.1. Optional state machine parameter configuration

- Configure the msgTxHold parameter of the LLDP interface

Command	SWITCH(lldp-agent)# **lldp msg-tx-hold** <1-100> SWITCH(lldp-agent)# **no lldp msg-tx-hold**
Description	LLDP interface proxy configuration mode. This variable is used as a multiplier for msgTxInterval to determine the value of txTTL carried in LLDP frames transmitted by the LLDP proxy. The default msgTxHold is 4. Administrators can change this value to any value in the range 1 to 100. TTL=msgTxInterval * msgTxHold + 1. Optional.

- Configure the txFastInit parameter of the LLDP interface

Command	SWITCH(lldp-agent)# **lldp tx-fast-init** <1-8> SWITCH(lldp-agent)# **no lldp tx-fast-init**
Description	LLDP interface proxy configuration mode. This variable is used as the initial value of the txFast variable. This value determines the number of LLDPDUs transmitted during the fast transmission period. The default value of txFastInit is 4. Administrators can change this value to any value between 1 and 8. Optional.

- Configure the txCredit parameter of the LLDP interface

Command	SWITCH(lldp-agent)# **lldp tx-max-credit** <1-8> SWITCH(lldp-agent)# **no lldp tx-max-credit**

Description	LLDP interface proxy configuration mode. Configure the maximum value of txCredit. The default value is 5. Administrators can change this value to any value in the range 1 to 10. Optional.

- Configure the msgFastTx parameter of the LLDP interface

Command	SWITCH(lldp-agent)# **lldp timer msg-fast-tx** <1-3600> SWITCH(lldp-agent)# **no lldp timer msg-fast-tx**
Description	LLDP interface proxy configuration mode. This variable defines the time interval of the timer interval between two transfers in a fast transfer period (ie txFast is not zero). The default value for msgFastTx is 1; administrators can change this value to any value between 1 and 3600. Optional.

- Configure the msgTxInterval parameter of the LLDP interface

Command	SWITCH(lldp-agent)# **lldp timer msg-tx-interval** <5-3600> SWITCH(lldp-agent)# **no lldp timer msg-tx-interval**
Description	LLDP interface proxy configuration mode. This variable defines the timer interval between normal transfers (ie, txFast is zero). The default value of msgTxInterval is 30 s; administrators can change this value to any value between 5 and 3600. Optional.

- Configure the reinitDelay parameter of the LLDP interface

Command	SWITCH(lldp-agent)# **lldp timer reinit-delay** <1-10> SWITCH(lldp-agent)# **no lldp timer reinit-delay**
Description	LLDP interface proxy configuration mode. This parameter represents the amount of delay between when adminStatus becomes "disabled" and when reinitialization is attempted. The default value of reinitDelay is 2 s.

	Optional.

1.2.1. Send tlv list configuration

- Configure the tlv selection of the LLDP interface

Command	SWITCH(lldp-agent)# [**no**] **lldp tlv-select basic-mgmt** { management-address | port-description | system-capabilities | system-description | system-name} SWITCH(lldp-agent)# [**no**] **lldp tlv-select ieee-8021-org-specific** {link-agg | mgmt-vid | port-ptcl-vlanid | port-vlanid | ptcl-identity | vid-digest | vlan-name} SWITCH(lldp-agent)# [**no**] **lldp tlv-select ieee-8023-org-specific** { mac-phy | max-mtu-size}
Description	LLDP interface proxy configuration mode. Multiple tlvs can be selected with multiple commands. Optional. Note: When there are many VLAN configurations on the device, the VLAN-related tlv may cause the packet length to exceed the MTU, resulting in packet sending errors. It is necessary to configure not to send this type of tlv.

1.3. Configuration case

1.3.1.LLDP basic function configuration example

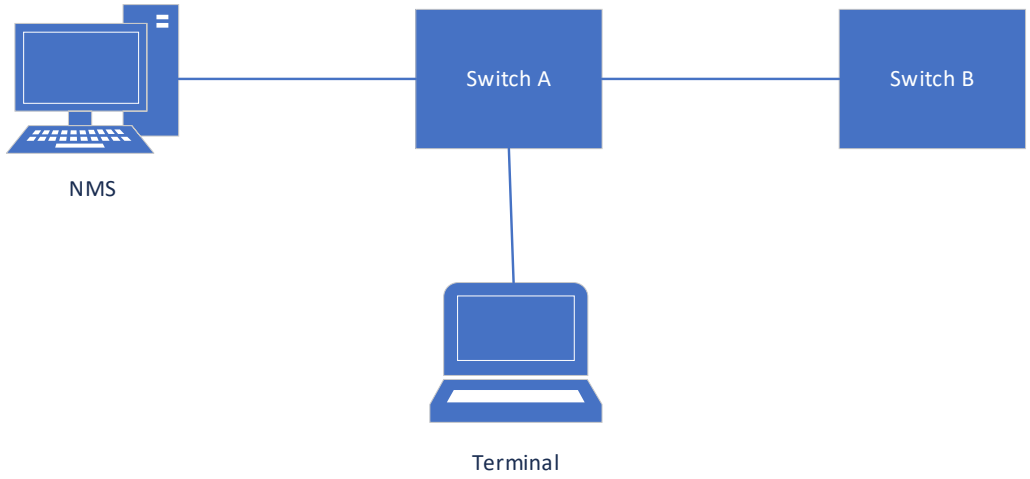
Networking requirements

The NMS (Network Management System, network management system) is connected to Switch A, and Switch A is connected to the Terminal device and Switch B respectively.

By configuring the LLDP function on Switch A and Switch B, the NMS can judge the communication status of the link between Switch A and the terminal device, and between Switch A and Switch B.

Network diagram

Diagram 22-1 LLDP Basic function configuration network diagram



Typical configuration eg.

Switch A/B:

```
Lldp run
```

1.3. DISPLAY COMMAND

- Display the status of LLDP interface

```
#show lldp interface gigabitEthernet0/2

Agent Mode : Nearest bridge
Enable (tx/rx): Y/Y
Message fast transmit time:1
Message transmission interval:30
Reinitialisation delay:2
MED Enabled :Y
Device Type: NOT_DEFINED
LLDP Agent traffic statistics:
Total frames transmitted: 4608
Total entries aged: 0
Total frames received: 150
Total frames received in error: 0
Total frames discarded: 0
Total discarded TLVs: 0
Total unrecognised TLVs: 0
```

- Display LLDP interface neighbors

```
#show lldp interface gigabitEthernet0/2 neighbor
 Nearest bridge Neighbors
Interface Name      : gigabitEthernet0/2
System Name         :
```

```
System Description  :
Port Description    :
TTL                 : 3601
System Capabilities : Routing
 Mandatory TLVs :
  CHASSIS ID TYPE :
   Chassis MAC Address: 000e.c6c1.3841
  PORT ID TYPE :
   Port MAC Address: 000e.c6c1.3841
8021 ORIGIN SPECIFIC TLV
 Port Vlan id  :0
 PP Vlan id    :0
 Remote Protocols Advertised  :
 Remote VID Usage Digest  : 0
 Remote Management Vlan   : 0
 Link Aggregation Status  : Disabled
 Link Aggregation Port ID : 0
8023 ORIGIN SPECIFIC TLV
 AutoNego Support     :  Supported Enabled
 AutoNego Capability  : 1
 Operational MAU Type : 0
 Max Frame Size       : 0
 MED Capabilities  :  Capabilities
 MED Capabilities Dev Type : End Point Class-1
 MED Application Type : Reserved
 MED Vlan id : 0
 MED Tag/Untag: Untagged
 MED L2 Priority : 0
 MED DSCP Val : 0
```

14. CONFIGURE L3

14.1. L3 OVERVIEW

L3 functions include Layer 3 port management, ARP management and routing management. Routing management does not include dynamic routing management.

- Layer 3 port management:

Layer 3 ports are for Layer 2 (switching) ports, and are generally divided into routing ports (ordinary physical ports or aggregation ports switched to Layer 3 ports) or SVI ports (Switch Virtual Interface, corresponding to a VLAN). The SVI port is a logical interface built on top of all the member ports included in the corresponding VLAN. Different from the routing port, the packets that are forwarded at Layer 3 through the SVI will first pass through Layer 2 (such as VLAN filtering, address learning, etc.)) and then go through three layers, and then go through three layers and then two layers when outputting (such as VLAN output rules).

The Internet Protocol (IP) uses logical virtual addresses to send data packets from source to destination, namely IP addresses. At the network layer, routing devices use IP addresses to complete packet forwarding. (Protocol specification: RFC 1918: Address Allocation for Private Internets, RFC 1166: Internet Numbers)

Layer 3 port management also includes IP address maintenance for Layer 3 ports. An IP address is composed of 32-bit binary. For the convenience of writing and description, it is generally expressed in dotted decimal. When expressed in dotted decimal, it is divided into four groups, each with 8 digits, ranging from 0 to 255. The groups are separated by ".", for example, "192.168.1.1" is the IP address expressed in decimal. The IP address, as the name suggests, is naturally the interconnection address of the IP layer protocol. A 32-bit IP address consists of two parts: 1) the network address part, which indicates which network it is; 2) the host address part, which indicates which host in the network. The network address part and the host address address part of the IP address are divided by the network mask. The network mask is also a 32-bit value consisting of several bits "1" in the front and several bits "0" in the back. The IP address is related to the network. The mask and the obtained is the corresponding part of the network address. Likewise, the netmask can also be directly represented by the mask length. For example, "192.168.1.1 255.255.255.0" and "192.168.1.1/24" represent the same IP address.

The Layer 3 interface of the device does not support the configuration of the second IP address

，That is, a Layer 3 interface can be configured with at most one IP address. When a Layer 3 port is configured with an IP address, a network segment is determined. Different Layer 3 ports of the same device must belong to different network segments, and IP addresses configured with different Layer 3 ports must belong to different network segments. The Layer 3 port represented by the SVI, and the corresponding VLAN is used as the unique identifier of the Layer 3 port.

After the different Layer 3 ports of the device are divided into different network segments, the forwarding between these different network segments (such as VLAN1 and VLAN2) is called "Layer 3 forwarding" (across network segments, or across different VLANs).

- ARP management：

In a local area network, each IP network device has two addresses: 1) the local address, since it is included in the frame header of the data link layer, it should be more precisely the data link layer

address, but in fact, it is the local address. The address is processed by the MAC sublayer in the data link layer, so it is habitually called the MAC address. The MAC address represents the IP network device on the local area network; 2) The network address represents the IP network device on the Internet. The network to which the device belongs is also stated.

To communicate between two IP devices on the LAN, they must know each other's 48-bit MAC address. The process of learning the MAC address from the IP address is called address resolution. There are two types of address resolution methods: 1) Address Resolution Protocol (ARP); 2) Proxy Address Resolution Protocol (Proxy ARP). About ARP and Proxy ARP, they are described in RFC 826 and RFC 1027 documents respectively.

ARP (Address Resolution Protocol, Address Resolution Protocol) is used to bind a MAC address and an IP address. Taking the IP address as an input, ARP can know its associated MAC address. Once the MAC address is known, the IP address to MAC address correspondence is stored in the device's ARP cache. With the MAC address, the IP device can encapsulate the link layer frame, and then send the data frame to the LAN. The encapsulation of IP and ARP on Ethernet is Ethernet II type.

ARP entries are divided into two categories: dynamic entries generated by the ARP protocol and static entries derived from static configuration. The dynamic ARP entry is formed by triggering the opening of the IP packet. The opening process is an ARP request/response process. If the ARP entry formed after the opening is unreachable, it will automatically age out. Static ARP entries do not need to be opened and will not age.

- Routing management:

Routing management is responsible for managing routing tables, integrating routes issued by various routing protocols, and performing optimization. According to different sources, the routing table is usually divided into the following three categories:

- Direct route: The route discovered by the link layer protocol is also called the interface route. A direct route is automatically generated when an IP address is configured on a Layer 3 port, and the route prefix is the network directly connected to the Layer 3 port.
- □Static routing: manually configured by the network administrator.
- □Dynamic routing: routes discovered by dynamic routing protocols (such as RIP, OSPF).

This device does not support dynamic routing protocols and therefore does not support dynamic routing.

A routing table entry consists of two parts:

- Prefix: It is represented by an IP address and network mask (or mask length), which refers to the destination network or host determined by the routing table entry (when the mask length is 32, it means the host).

- Direct connection or next hop: Direct connection indicates that the destination network or host belongs to the directly connected network, and the direct connection route belongs to this situation. When configuring a static route, specifying a Layer 3 port instead of an IP address will also generate such a routing table entry. ; The next hop is represented by an IP host address, indicating that to reach the destination network or host, it needs to be forwarded to the IP network device indicated by the IP address.

When forwarding IP packets according to the routing table entry, if the routing table entry specifies the next hop, when the link layer encapsulates the ARP query, the IP of the next hop is used, that is, the destination MAC address of the link layer encapsulation is the next hop. The destination MAC address of the hop. If the routing table entry is directly connected, the destination IP address of the packet is directly used for ARP query, that is, the destination MAC address encapsulated at the link layer is the final destination MAC address of the packet. Either way, if the ARP query fails, the route will be opened (a dynamic ARP entry will be generated). If the connection cannot be made, the IP packet cannot be forwarded and will be discarded.

There may be an inclusion relationship between routing table entries (depending on the length of the mask), so the route lookup process satisfies the LPM (Longest Prefix Match, longest prefix match). That is, when IP packets are forwarded for route lookup, if multiple routing entries are hit at the same time, the routing entry with the longest prefix mask length is selected.

14.2. CONFIGURE COMMAND

14.2.1. Configure/Delete SVI Port IP Address

Command	Configure the IP address of the Layer 3 port: SWITCH(config)#int vlan10 SWITCH(config-if)#**ip address** IPADDR/MASKLEN OR: SWITCH(config-if)#**ip address** IPADDR MASK Delete the IP address of the Layer 3 port: SWITCH(config)#int vlan10 SWITCH(config-if)#**no ip address** IPADDR/MASKLEN Or SWITCH(config-if)#**no ip address** IPADDR MASK Check the IP address of the Layer 3 port: SWITCH#**show ip interface brief**

Description	Configure in the interface mode of the SVI. When a VLAN is created, the SVI is automatically created, and when the VLAN is deleted, the SVI is automatically deleted. int vlanXX is to enter the interface mode of the SVI instead of creating an SVI port. Therefore, when the SVI does not exist (the corresponding VLAN does not exist), entering the interface mode of the SVI will fail. At the same time, when the SVI is deleted, the IP address configured on it will be automatically cleared. Layer 3 ports support IP address configuration update, which has the same effect as deleting and reconfiguring. The IP addresses configured on different Layer 3 ports must belong to different network segments. Layer 3 ports do not support second ip configuration. Note: After this command is configured, the system will clear the management IP configuration (refer to: Configuring Management IP), and use the Layer 3 port IP address as the device management IP instead.

14.2.1. Configure/Delete IP Address of Routing Port

Command	Configure the IP address of the routing port:
	SWITCH(config)#**interface** gigabitEthernet0/1
	SWITCH(config-if)#**no switchport**
	SWITCH(config-if)#**ip address** IP(A.B.C.D/M)
	Or
	SWITCH(config-if)#ip address IP(A.B.C.D) MASK(A.B.C.D)
	
	Delete the IP address of the Layer 3 port:
	SWITCH(config)# interface gigabitEthernet0/1
	SWITCH(config-if)#no ip address IP(A.B.C.D/M)
	Or
	SWITCH(config-if)#no ip address IP(A.B.C.D) MASK(A.B.C.D)
	SWITCH(config-if)#switchport

Description	Configure in interface mode. Before configuring the routing port IP, since the default attribute of the interface is the Layer 2 port attribute, you need to use the no switchport command to switch the port from the Layer 2 port attribute to the Layer 3 routing port attribute, and then use the ip address command to configure the routing port attribute. IP configuration, otherwise, switch the routing port to the Layer 2 port attribute, use the switchport command. Layer 3 ports support IP address configuration update, which has the same effect as deleting and reconfiguring. The IP addresses configured on different Layer 3 ports must belong to different network segments. Layer 3 ports do not support second ip configuration.

14.2.1. Configuring/deleting static ARP entries

Command	SWITCH(config)#**arp** IPADDR MACADD SWITCH(config)#**no arp** IPADDR

Description	Configure in global configuration mode. The IP address configured with static ARP must belong to the directly connected network segment, otherwise the configuration fails. Static ARP has a higher priority than dynamic ARP. When the two conflict, static ARP takes effect. When the IP address of the Layer 3 port is deleted or the Layer 3 port is deleted, if the IP address of the static ARP belongs to the directly connected network segment of the Layer 3 port, the static ARP will be invalid (you can see that the entry does not exist through show arp, but show run, you can see that the configuration is still there); Similarly, when a Layer 3 port is configured with an IP address, the ARP entry of the directly connected network segment whose IP address belongs to the Layer 3 port will change from an invalid state to a valid state. (You can see the existence of ARP entries through show arp).

14.2.1. Clear the ARP cache

command	SWITCH#**clear arp-cache**
Description	Clear the ARP cache in privileged mode. This command only clears dynamic ARP entries, and static ARP entries will not be cleared.

14.2.1. Configuring/deleting static routes

Command	SWITCH(config)#**ip route** {IPADDR/MASKLEN) | IPADDR MASK} {NH_IPADDR | IFNAME} SWITCH(config)#**no ip route** {IPADDR/MASKLEN | IPADDR MASK} {NH_IPADDR | IFNAME}
Description	Configure in global configuration mode. Recursive routing is not supported (the configured next-hop IP must belong to the directly connected network segment); The route prefix cannot belong to the directly connected network segment (that is, the directly connected route is automatically generated and cannot be statically configured).

	When a Layer 3 port is configured with an IP address, if the prefix of a static routing entry belongs to the directly connected network segment of the Layer 3 port, the static route will be automatically deleted and a LOG prompt will be displayed; When the IP address of a Layer 3 port is deleted or the Layer 3 port is deleted, if the next hop IP of a static routing entry belongs to the directly connected network segment of the Layer 3 port, the static route is automatically deleted and a LOG prompt is displayed.

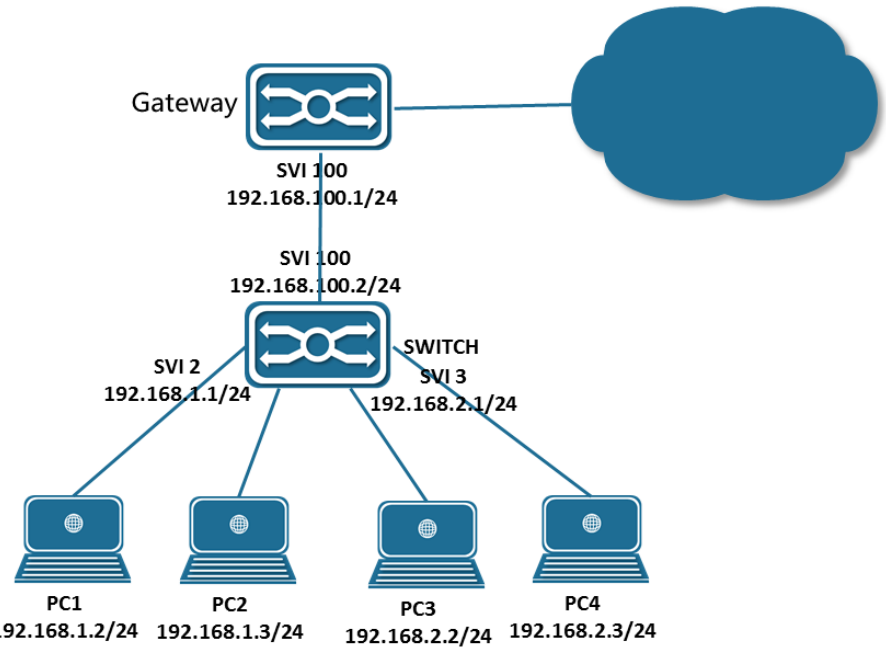
14.2.1. Configuring ECMP Policy

If there are redundant links in the network environment, that is, there are multiple next hops for the route to the same destination address. On devices that support ECMP technology, multiple next hops can work at the same time, so that redundant links can be fully utilized, and when a link failure occurs on a redundant link, traffic can be switched to other redundant links. Network reliability and stability.

ECMP (Equal-Cost Multipath Routing, Equal Cost Routing), this technology enables the device to use multiple next-hop links of the corresponding route concurrently, and balance the traffic among the multiple next-hop links according to the set balance factor distribution; and supports fast switchover of faulty links.

14.3. CONFIGURE CASE

Case 1 ： Weak Layer 3 Gateway



As a weak Layer 3 gateway, the Switch reduces the ARP burden for the real gateway.

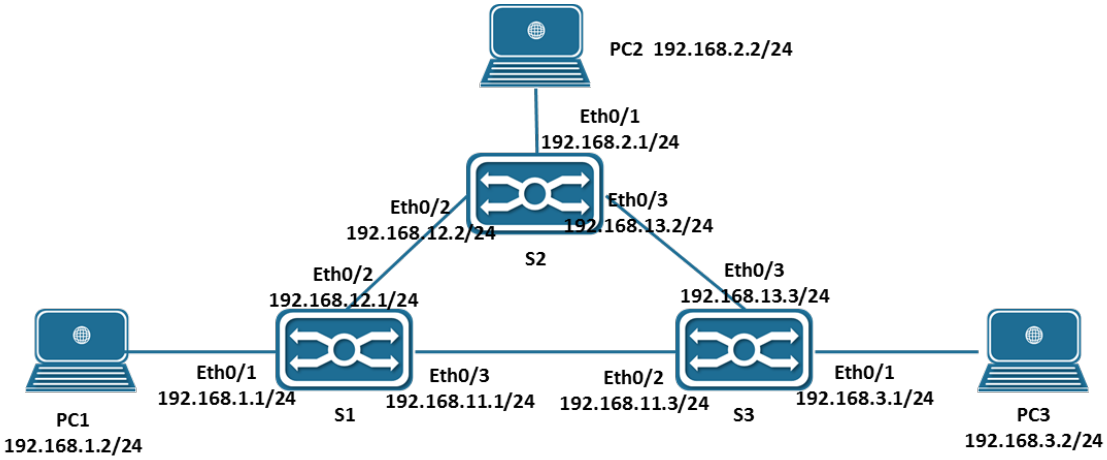
- Configuring the PC:
- □PC1, PC2 and PC3 configure IP addresses as shown in the figure, and specify the gateway at the same time. For example, the gateway of PC1 and P2 is 192.168.1.1.
- □Configure SWITCH:
  - Configure the Layer 3 port and IP address: (Assume that the interface connecting PC1-PC4 is gigabitEthernet0/1-4, and the uplink interface is gigabitEthernet0/17)

```
SWITCH(config)#vlan 2-3,100
SWITCH(config)#interface gigabitEthernet0/1-2
SWITCH(config-if)#switch access vlan 2
SWITCH(config)#interface gigabitEthernet0/3-4
SWITCH(config-if)#switch access vlan 3
SWITCH(config)#interface gigabitEthernet0/17
SWITCH(config-if)#switch access vlan 100
SWITCH(config)#int vlan2
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config)#int vlan3
SWITCH(config-if)#ip address 192.168.2.1/24
SWITCH(config)#int vlan100
SWITCH(config-if)#ip address 192.168.100.2/24
```

  - Configure static route (default route):

```
SWITCH(config-if)ip route 0.0.0.0/0 192.168.100.1
```

Case 2: Intranet Layer 3 Interconnection



In the network environment shown above, PC1, PC2 and PC3 are interconnected through S1, S2 and S3 respectively.

- Configure the PC

- □PC1, PC2 and PC3 configure IP addresses as shown in the figure, and specify the gateway at the same time. For example, the gateway of PC1 is 192.168.1.1.
- □Configure S1
  - ➢ □Configure the Layer 3 port and IP address:

```
SWITCH(config)#vlan 2-4
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#switch access vlan 2
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#switch access vlan 3
SWITCH(config)#interface gigabitEthernet0/3
SWITCH(config-if)#switch access vlan 4
SWITCH(config)#int vlan2
SWITCH(config-if)#ip address 192.168.1.1/24
SWITCH(config)#int vlan3
SWITCH(config-if)#ip address 192.168.12.1/24
SWITCH(config)#int vlan4
SWITCH(config-if)#ip address 192.168.13.1/24
```

  - ➢ Configure static routes

```
SWITCH(config)#ip route 192.168.2.0/24 192.168.12.2
SWITCH(config)#ip route 192.168.3.0/24 192.168.11.3
```

- S2 and S3 are similar to the configuration of S1.

14.4. DISPLAY COMMAND

- Display ARP entries

```
SWITCH#show arp
Address                  HWaddress              Interface      Type
192.168.1.238         00:00:00:00:04:86       vlan2          Static
192.168.2.46           00:00:00:00:05:45       vlan3          Static
192.168.3.110         00:00:00:00:08:59       vlan4          Static
192.168.0.12           00:00:00:00:00:09       vlan1          Static
192.168.0.1             00:0e:c6:d8:c7:f7         vlan1          Dynamic
10.100.2.2              00:01:a0:00:10:11       GiE0/2         Dynamic
```

- Display routing table entries

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS
inter area
          * - candidate default
       IP Route Table for VRF "default"
       Gateway of last resort is 192.168.1.3 to network 0.0.0.0
       S*      0.0.0.0/0 [1/0] via 192.168.1.3, vlan2
       S       192.168.0.0/16 [1/0] via 192.168.0.10, vlan1
       C       192.168.0.0/24 is directly connected, vlan1
       C       192.168.1.0/24 is directly connected, vlan2
       C       192.168.2.0/24 is directly connected, vlan3
       C       192.168.3.0/24 is directly connected, vlan4
       C       10.100.2.0/30 is directly connected, gigabitEthernet0/2
```

15. CONFIGURE OSPFV2

15.1. OSPFV2 OVERVIEW

OSPF (Open Shortest Path First) is a link-state-based interior gateway routing protocol developed by the IETF OSPF working group.

OSPF is a routing protocol specially developed for IP. It runs directly on the IP layer, the protocol number is 89, and the OSPF packet exchange is carried out in the multicast mode. The multicast addresses are 224.0.0.5 (all OSPF devices) and 224.0.0.6 (specified devices) . It is applied inside AS (Autonomous System, autonomous system).

A group of devices running the OSPF routing protocol constitute the autonomous domain system of the OSPF routing domain.

An autonomous domain system refers to all the devices controlled and managed by an organization. Only one IGP routing protocol runs in the autonomous domain system. The BGP routing protocol is usually used to exchange routing information between autonomous domain systems. Different autonomous domain systems can choose the same IGP routing protocol. If they want to connect to the Internet, each autonomous domain system needs to apply for the autonomous domain system number from the relevant organization.

When the OSPF routing domain is large, a hierarchical structure is generally adopted, that is, the OSPF routing domain is divided into several areas, and the areas are interconnected through a backbone area, and each non-backbone area needs to be directly connected to the backbone area.

In an OSPF routing domain, there are three device roles depending on where the device is deployed:

- Intra-area equipment: All interface networks of the equipment belong to one area;
- Area Border Routers: ABR (Area Border Routers). The interface network of the device belongs to at least two areas, one of which must be the backbone area.
- Autonomous domain boundary device: ASBR (Autonomous System Boundary Routers), is the only way for the OSPF routing domain to exchange routes with external routing domains.

The link state algorithm is a completely different algorithm from the Huffman vector algorithm (distance vector algorithm). The traditional routing protocol using the Huffman vector algorithm is RIP, while the OSPF routing protocol is a typical implementation of the link state algorithm. Compared with the RIP routing protocol, in addition to the algorithm difference, OSPF also introduces new concepts such as routing update authentication, VLSMs (variable-length subnet masks), and route aggregation. The RIP protocol has two fatal weaknesses: slow convergence speed and limited network size (the maximum number of hops does not exceed 16). OSPF overcomes the weaknesses of RIP and can be used in medium-to-large and complex network environments.

The OSPF routing protocol uses the link state algorithm to establish and calculate the shortest path to each target network. The algorithm itself is relatively complex. The following briefly describes the overall process of the link state algorithm:

- In the initialization phase, the device will generate a link status advertisement, which contains all the link status of the device;

- □ All devices exchange link status information through multicast. When each device receives a link status update message, it will copy a copy to the local database, and then spread it to other devices;
- □ When each device has a complete link state database, the device applies Dijkstra algorithm to calculate the shortest path tree for all target networks. The result includes: target network, next hop address, cost, which is a key part of the IP routing table .

If there is no link cost, network addition or deletion changes, OSPF will be very quiet. If there is any change in the network, OSPF will advertise through the link state, but only the changed link state will be advertised, and the devices involved in the change will re-run the Dijkstra algorithm. , to generate a new shortest path tree.

15.2. CONFIGURE COMMAND

15.2.1. Create OSPF process

Command	SWITCH(config)#**router ospf** *process-id* SWITCH(config-router)#**router-id** *router-id* SWITCH(config-router)# **network** *IP(A.B.C.D) MASK(A.B.C.D)* **area** *area-id*
Description	To run the OSPF routing protocol, you need to create an OSPF routing process and associate the corresponding network with the OSFP routing process. The router router command is to create an OSPF routing process. The process-id is the instance number of the OSPF routing process. If it is not configured, it means process instance 1. The router-id command is used to set the ID of the routing device, expressed in the form of an IP address. Each OSPF process uses a different Router ID to distinguish. The network command indicates the routing information of the associated network advertised by the OSPF command, and also indicates that the protocol advertisement and routing information update are performed only on the interface corresponding to the associated network. IP and MASK together form the address range. area-id is the OSPF area identifier, which is always associated with an IP address range. Usually, for the convenience of management, the subnet mask is used as the OSPF area identifier.

15.2.2. Interface Network Type Configuration

Command	SWITCH(config-if)#**ip ospf network** {broadcast|non-broadcast|point-to-multipoint [non-broadcast]|point-to-point}
Description	broadcast indicates the broadcast type. It sends OSPF packets in multicast mode, can automatically discover neighbors, and elect DR (Designated Router) and BDR (Backup Designated Router). non-broadcast means sending OSPF packets in unicast mode. In this type, you need to manually specify the neighbor address and elect the DR and BDR. The devices are fully meshed, and the interconnected devices can communicate directly.

	point-to-multipoint: This type does not require a full mesh connection and can be regarded as multiple P2P links, so multiple host routes will be generated. This type does not perform DR/BDR elections, and metric values can be set for each neighbor. (without non-broadcast): Send OSPF packets in multicast mode to automatically discover neighbors. (with non-broadcast): To send OSPF packets in unicast mode, you need to manually specify neighbors. Point-to-point indicates a point-to-point connection, requiring interfaces to be interconnected in a 1-to-1 mode, sending OSPF packets in multicast mode, and automatically discovering neighbors without DR/BDR election.

Command	SWITCH(config-if)#**ip ospf priority** *priority*
Description	priority is used to specify the priority of the interface. The larger the value, the higher the priority. The default is 1.

DR（Designated Router）：Specifies the router.
BDR（Designated Router）：Backup the designated router.
In an OSPF network, only the DR device advertises the link status of the network, and all other devices maintain the neighbor relationship, but all devices only maintain the adjacency relationship with the DR/BDR, that is, the devices other than the DR/BDR only communicate with the DR /BDR devices exchange link state data packets, and DR summarizes and calculates them and then advertises them to other devices. OSPF protocol uses this mechanism to ensure that the link state data of all devices in the network are consistent.
The DR is elected by comparing the interface priorities. The device with the highest priority is elected as the DR device, and the device whose priority is set to 0 is the device that gives up the election qualification. If OSPF neighbors do not receive DR hello packets within a certain period of time, they will consider that the DR is down and will initiate a new round of DR election. This is the only condition for DR election. The device's dynamic priority modification does not take effect immediately, and only takes effect when a new round of election is triggered.

15.2.2. Specifying neighbor configuration

Command	SWITCH(config-router)#**neighbor ip-address** [cost cost-value] [priority *priority-value*] [poll-interval *seconds*]
Description	ip-address indicates the ip address of the neighbor. cost represents the metric value of the interface to the neighbor. Only valid when the interface type is point-to-multipoint. priority indicates the priority of the neighbor. The larger the value, the higher the priority. The default is 0. Valid when the interface type is non-broadcast. poll-interval indicates the interval for sending hello packets to a neighbor in the down state. The default value is 120 seconds. Valid when the interface type is non-broadcast.

15.2.2. Protocol Control Configuration

- Configure the hello packet interval

Command	SWITCH(config-if)#**ip ospf hello-interval** *seconds*
Description	hello-interval is used to set the interval for sending hello packets on the interface. The value of the two ends of the neighbor must be the same.

- Configure the dead judgment interval

Command	SWITCH(config-if)#**ip ospf dead-interval** *seconds*
Description	dead-interval seconds is used to set the time interval for determining the death of a neighbor on the interface. The values on both ends of the neighbor must be the same

- Configure OSPF to advertise mtu

Command	SWITCH(config-if)#**ip ospf mtu** *mtu-value*
Description	mtu is used to set the mtu value of the interface advertised by OSPF.

- Disable mtu verification

Command	SWITCH(config-if)#**ip ospf mtu-ignore**
Description	mtu-ignore is used to set the MTU check to disable OSPF. The OSPF protocol will check the MTU of the neighbor interface when receiving the database description packet. If the MTU of the interface indicated in the receiving database description packet is greater than the MTU of the receiving interface, the adjacency relationship cannot be established. In this case, except for modifying the mtu value In addition, you can also use this configuration to turn off mtu verification to solve the problem.

- LSA is prohibited

Command	SWITCH(config-if)#**ip ospf database-filter all out**
Description	mtu-ignore is used to set the MTU check to disable OSPF. The OSPF protocol will check the MTU of the neighbor interface when receiving the database description packet. If the MTU of the interface indicated in the receiving database description packet is greater than the MTU of the receiving interface, the adjacency relationship cannot be established. In this case, except for modifying the mtu value In addition, you can also use this configuration to turn off mtu verification to solve the problem.

- Configure the delay of sending lsu packets

The LSU packet contains the Age field of LSAs (link state description), and this field will be incremented before the LSU packet is sent. When the Age reaches 3600, the lsu packet will be retransmitted or requested to be retransmitted. If it is not refreshed in time, the expired LSA will be deleted from the link state database. For low-speed lines, due to the large delay in interface transmission and line propagation, the Age field needs to be incremented faster. In this case, the delay in sending lsu packets needs to be increased, and the increment step of the Age field needs to be increased to trigger retransmission.

Command	SWITCH(config-if)#**ip ospf tramsmit-delay** *seconds*
Description	transmit-delay is used to set the delay of lsu packets on the interface, in seconds.

- Configure the retransmission interval of lsu packets

After the device sends an lsu packet, the lsu packet may not be delivered due to various reasons or may not receive an acknowledgment response from the other party. In this case, the lsu packet needs to be retransmitted. Set the retransmission interval by configuring the lsu packet retransmission interval. transmission time.

Command	SWITCH(config-if)#**ip ospf retransmit-interval** *seconds*
Description	retransmit-interval is used to set the retransmission interval of lsu packets on the interface, in seconds. The time needs to be greater than the round-trip transmission delay of data packets between neighbors.

- Configure the SPF refresh delay

Command	SWITCH(config-router)#**timers spf spf-delay** *spf-holdtime*
Description	spf-delay indicates the delay time from the change of network topology to the start of SPF calculation, which is used to set the sensitivity of SPF calculation to the perception of network topology changes. spf-holdtime indicates the minimum time interval from the first trigger of SPF calculation to the second trigger of SPF calculation.

If link flapping occurs only occasionally, set the spf-delay and spf-holdtime to a small value to speed up the OSPF convergence speed; set a large value to prevent the link from flapping rapidly and consume a large amount of CPU resources.

15.2.2. Passive interface configuration

Passive interface configuration can be used to prevent the routing information of the device from being learned by other devices. It can be set based on the whole machine or the passive interface and address of the specified interface device. Passive interfaces/passive addresses cannot establish neighbors and cannot exchange OSPF packets, but the routing information of passive addresses can be advertised through non-passive addresses and learned by neighbors

Command	SWITCH(config-router)#**passive-interface default** SWITCH(config-router)#**passive-interface** *interface-name* SWITCH(config-router)#**passive-interface** *interface-name ip-address* SWITCH(config-router)#**no passive-interface** *interface-name*
Description	default means that all interfaces are set as passive interfaces. interface-name indicates that the specified interface is configured as a passive interface. ip-address means to configure a passive address. no means to delete the passive interface.

15.2.2. Default route advertisement configuration

Command	SWITCH(config-router)#**default-information originate** [always] [metric metric] [metric-type *type*] [route-map *map-name*]
Description	always means that OSPF will unconditionally generate a default route regardless of whether there is a default route locally. metric indicates the metric value of the default route. metric-type indicates the type of the default route. There are two types of external routes in OSPF: the external routes of type 1 have different metric values on different routing devices; the external routes of type 2 have the same metric value on all routing devices. map-name indicates the map associated with route-map.

After the default-information originate command is configured, the device will automatically become an ASBR.

The ABR in the STUB area will automatically advertise the default route to the STUB area.

The ABR in the NSSA area will automatically advertise the default route to the NSSA area.

15.2.2. Route Republishing Configuration

Command	SWITCH(config-router)# **redistribute** {bgp | connected | isis [area-tag] | ospf process-id | rip | static} [metric *value*] [metric-type {1 | 2}] [route-map *map-name*] [subnets] [tag *value*]
Description	This command is used to configure the import of external routes (including other OSPF processes/static routes/routes of other routing protocols) to the OSPF process on the ASBR.

15.2.2. Route aggregation configuration

- Configuring inter-area route aggregation

Command	SWITCH(config-router)#**area area-id range** *ip-address/mask* [advertise|not-advertise]
Description	area-id indicates the OSPF area id of route aggregation. ip-address and mask indicate the network segment IP and mask of the aggregation route. advertise and not-advertise indicate whether the aggregation route needs to be advertised.

This command is only valid on ABR devices. The function is to merge and aggregate multiple routes in the area into one route and then advertise it to other areas. Since the aggregation occurs only on the ABR device, the routes inside the area see specific routing information, but other devices outside the area can only see the aggregated route. Multiple area aggregation routes can be defined at the same time. Route aggregation can simplify the routing of the entire routing domain.

- Configuring external route aggregation

Command	SWITCH(config-router)#**summary-address** *ip-address mask* [not-advertise|tag *tag-value*]
Description	area-id indicates the OSPF area id of route aggregation. ip-address and mask indicate the network segment IP and mask of the aggregation route. not-advertise means not to advertise the aggregated route, if this parameter is not used, it means to advertise. tag-value indicates the tag value of the route.

The routes advertised by other routing processes to the OSPF routing process are advertised to OSPF in the form of external link states. If the injected routes are in a continuous address space, the AS domain convenient device routing device can aggregate multiple routes in the continuous address space. It can be advertised as a route, which can reduce the size of the routing table of the routing device in the domain.
When summary-address is configured on the ABR in the NSSA domain, only redistributed routes and LSA class 7 to class 5 routes are aggregated. When the summary-address is configured on the ASBR, only redistributed routes are aggregated.
The difference between the summary-address and the area range is that the area range aggregates the routes within the OSPF area, and the summary-address aggregates the routes outside the OSPF area.

15.2.2. Shortest Path Configuration

- Configure the metric value of the outbound direction of the interface

There are three ways to configure the metric value in the outbound direction of an interface:

- One is to use the ratio of the automatically calculated reference bandwidth to the interface bandwidth by configuring the reference bandwidth as the metric for the outbound direction of the interface. Assume that the interface bandwidth is 100Mbps, and we configure the reference bandwidth to be 1000Mbps, then the default cost value of the interface is 1000/100=10.

Command	SWITCH(config-router)#**auto-cost reference-bandwidth** *ref-bw*
Description	ref-bw represents the reference bandwidth.

- The other is to configure the metric value directly on the interface based on elements such as link bandwidth and delay.

Command	SWITCH(config-if)#**ip ospf cost** *cost-value*
Description	cost-value represents the metric value.

- For point-to-multipoint interfaces, you can configure metrics based on neighbors in router mode.

Command	SWITCH(config-router)#**neighbor ip-address** [cost *cost-value*]

Description	cost-value represents the metric value.

- Configure the default route metric value of STUB/NSSA area

  The default route metric sent by the ABR device to the STUB/NSSA area is 1 by default, and the metric can be specified by configuration.

Command	SWITCH(config-router)#**area** *area-id* **default-cost** *cost-value*
Description	area-id indicates the OSPF domain id. cost-value represents the metric value.

- Configure the default metric for republished routes

The default metric value of the BGP route re-advertised by the ASBR device is 1, and the default metric value of other re-advertised routes is 20. The metric value can be specified through configuration, but it needs to be used in conjunction with the redistribute command.

Command	SWITCH(config-router)#**default-metric** *metric-value*
Description	cost-value represents the metric value.

- Configure the route management distance value

The route administrative distance refers to the reliability of the route source. It is a value between 0 and 255. The larger the data, the lower the reliability. When selecting a route, OSPF will preferentially select a route with a small administrative distance, which means high reliability. routing. The default value of the OSPF administrative distance is 110.

Command	SWITCH(config-router)#**distance** {*distance* | ospf {intra-area distance|inter-area distance|external *distance*}}
Description	intra-area indicates intra-area routing. inter-area indicates inter-area routing. external represents an external route. distance represents a measure.

15.2.2. Protocol Authentication Configuration

Unsupported so far .

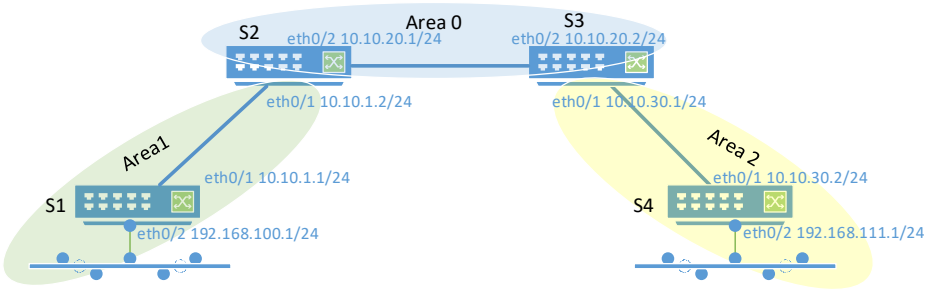
15.3. CONFIGURE CASE

15.3.1. **OSPF basic configuration**

Requirements

- 4 devices are configured with 3 areas in one autonomous domain;
- □The device runs the OSPF protocol;
- □Each device can learn all routes in the autonomous domain

Networking



Configure eg.

- Device S1 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/1
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.1.1/24
```

Configure the ip address of port gigabitEthernet0/2

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/2
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.100.1/24
```

Configure the OSPF process

```
S1(config)#router ospf 1
S1(config-router)#router-id 10.10.1.1
```

Associated Network

```
S1(config-router)#network 10.10.1.0 255.255.255.0 area 1
S1(config-router)#network 192.168.100.0 255.255.255.0 area 1
```

- Device S2 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/1
S2(config-if)#no switchport
S2(config-if)#ip address 10.10.20.1/24
```

Configure the ip address of port gigabitEthernet0/2

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/2
S2(config-if)#no switchport
S2(config-if)#ip address 10.10.10.1/24
```

Configure the OSPF process

```
S2(config)#router ospf 1
S2(config-router)#router-id 10.10.1.2
```

Associated Network

```
S2(config-router)#network 10.10.10.0 255.255.255.0 area 1
S2(config-router)#network 10.10.20.0 255.255.255.0 area 0
```

- Device S3 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/1
S3(config-if)#no switchport
S3(config-if)#ip address 10.10.20.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/2
S3(config-if)#no switchport
S3(config-if)#ip address 10.10.30.1/24
```

Configure the OSPF process

```
S3(config)#router ospf 1
S3(config-router)#router-id 10.10.20.2
```

Associated Network

```
S3(config-router)#network 10.10.20.0 255.255.255.0
S3(config-router)#network 10.10.30.0 255.255.255.0
```

- Device S4 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/1
S4(config-if)#no switchport
S4(config-if)#ip address 10.10.30.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/2
S4(config-if)#no switchport
S4(config-if)#ip address 192.168.111.1/24
```

Configure the OSPF process

```
S4(config)#router ospf 1
S4(config-router)#router-id 10.10.30.2
```

Associated Network

```
S4(config-router)#network 10.10.30.0 255.255.255.0 area 2
S4(config-router)#network 192.168.111.0 255.255.255.0 area 2
```

- Results display

Device S1:

Display routing table on device S1

```
S1#show ip ospf neighbor


OSPF process 1:
Neighbor ID     Pri   State           Dead Time   Address
Interface
10.10.1.2         1   Full/DR         00:00:31    10.10.1.2
GiE0/1

S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C        10.10.1.0/24 is directly connected, gigabitEthernet0/1
O IA     10.10.20.0/24 [110/2] via 10.10.1.2, gigabitEthernet0/1, 00:37:09
O IA     10.10.30.0/24 [110/3] via 10.10.1.2, gigabitEthernet0/1, 00:36:19
C        192.168.100.0/24 is directly connected, gigabitEthernet0/2
O IA     192.168.111.0/24 [110/4] via 10.10.1.2, gigabitEthernet0/1, 00:36:19

Gateway of last resort is not set
S1#
```

Device S2:

Display routing table on device S2

```
S2#show ip ospf neighbor


OSPF process 1:
Neighbor ID     Pri   State           Dead Time   Address
Interface
10.10.1.1         1   Full/BDR        00:00:36    10.10.1.1
GiE0/1
10.10.20.2        1   Full/DR         00:00:31    10.10.20.2
GiE0/2

S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
```

```
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default

IP Route Table for VRF "default"
C           10.10.1.0/24 is directly connected, gigabitEthernet0/1
C           10.10.20.0/24 is directly connected, gigabitEthernet0/2
O IA       10.10.30.0/24 [110/2] via 10.10.20.2, gigabitEthernet0/2, 00:38:36
O           192.168.100.0/24 [110/2] via 10.10.1.1, gigabitEthernet0/1, 00:45:08
O IA       192.168.111.0/24 [110/3] via 10.10.20.2, gigabitEthernet0/2, 00:38:36

Gateway of last resort is not set
S2#
```

Device S3:

Display routing table on device S3

```
S3#show ip ospf neighbor


OSPF process 1:
Neighbor ID      Pri    State                 Dead Time     Address
Interface
10.10.1.2          1    Full/BDR              00:00:34      10.10.20.1
GiE0/2
10.10.30.2         1    Full/DR               00:00:31      10.10.30.2
GiE0/1

S3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default

IP Route Table for VRF "default"
O IA       10.10.1.0/24 [110/2] via 10.10.20.1, gigabitEthernet0/2, 00:39:20
C           10.10.20.0/24 is directly connected, gigabitEthernet0/2
C           10.10.30.0/24 is directly connected, gigabitEthernet0/1
O IA       192.168.100.0/24 [110/3] via 10.10.20.1, gigabitEthernet0/2, 00:39:20
```

```
O          192.168.111.0/24 [110/2] via 10.10.30.2, gigabitEthernet0/1, 00:39:20

Gateway of last resort is not set
S3#
```

Device S4:

Display routing table on device S4

```
S4#show ip ospf neighbor

OSPF process 1:
Neighbor ID      Pri    State                Dead Time    Address
Interface
10.10.20.2         1    Full/BDR              00:00:39     10.10.30.1
GiE0/1

S4#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
O IA     10.10.1.0/24 [110/3] via 10.10.30.1, gigabitEthernet0/1, 00:39:51
O IA     10.10.20.0/24 [110/2] via 10.10.30.1, gigabitEthernet0/1, 00:39:51
C        10.10.30.0/24 is directly connected, gigabitEthernet0/1
O IA     192.168.100.0/24 [110/4] via 10.10.30.1, gigabitEthernet0/1, 00:39:51
C        192.168.111.0/24 is directly connected, gigabitEthernet0/2

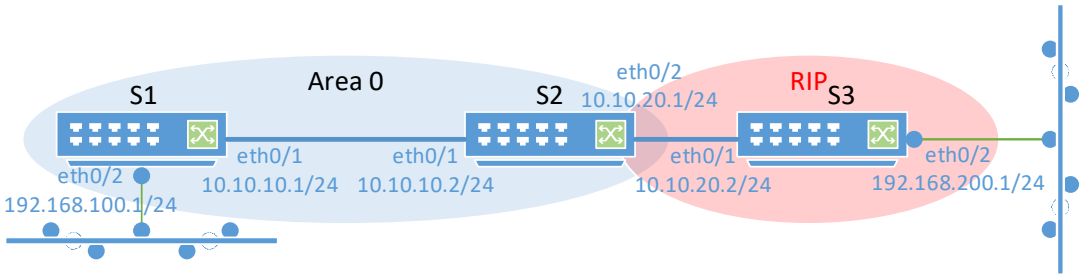
Gateway of last resort is not set
S4#
```

15.3.2.OSPF route redistribution configuration

Requirements

- area0 where S1 and S2 are in the same OSPF autonomous area
- S2 acts as an ASBR, exchanges routes with S3 through RIP, and distributes default routes and static routes to the AS domain
- S1, S2, S3 can learn each other's routes

Networking



Config. Case

- Device S1 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.1.1/24
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 192.168.100.1/24
```

Configure the OSPF process

```
SWITCH(config)#router ospf 1
```

Associated Network

```
SWITCH(config-router)#network 10.10.1.0 255.255.255.0 area 0
SWITCH(config-router)#network 192.168.100.0 255.255.255.0 area 0
```

- Device S2 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.1.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.20.1/24
```

Configure default and static routes

```
SWITCH#configure terminal
SWITCH(config)#ip route 0.0.0.0/0 10.10.20.2
SWITCH(config)#ip route 80.0.0.0/6 10.10.20.2
```

Configure the OSPF process and associate the network

S2 is the ASBR of OSPF, and needs to import the external routes advertised by RIP into the OSPF domain, that is, redistribute the routes of RIP to OSPF. You also need to configure static route redistribution and default route redistribution.

```
SWITCH(config)#router ospf 1
SWITCH(config-router)#network 10.10.1.0 255.255.255.0 area 0
SWITCH(config-router)#redistribute rip
SWITCH(config-router)#redistribute static
SWITCH(config-router)#default-information originate always
```

Configure the RIP process and associate the network

The routes between S2 and S3 are advertised through the RIP protocol. The routes in the OSPF domain need to be imported into the RIP process and then advertised to S3, that is, the OSPF routes are redistributed to RIP.

```
SWITCH(config)#router rip
SWITCH(config-router)#network 10.10.20.0 255.255.255.0
SWITCH(config-router)#redistribute ospf 1
```

- Device S3 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.20.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 192.168.200.1/24
```

Configure the RIP process and associate the network

```
SWITCH(config)#router rip
SWITCH(config-router)#network 10.10.20.0 255.255.255.0
SWITCH(config-router)#network 192.168.200.0 255.255.255.0
```

- Results display

Device S1

Display the routing table on device S1, you can see:

- ✧ The route of the 192.168.200.0/24 network segment learned from the external AS, that is, the RIP domain, learned through S2;
- ✧ Static route 80.0.0.0/6 learned through S2
- ✧ The default route learned through S2 is 0.0.0.0/0

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.10.1.2 to network 0.0.0.0

O*E2      0.0.0.0/0 [110/1] via 10.10.1.2, gigabitEthernet0/1, 4d00h19m
C         10.10.1.0/24 is directly connected, gigabitEthernet0/1
O E2      80.0.0.0/6 [110/20] via 10.10.1.2, gigabitEthernet0/1, 4d00h19m
C         192.168.100.0/24 is directly connected, gigabitEthernet0/2
O E2      192.168.200.0/24 [110/20] via 10.10.1.2, gigabitEthernet0/1,
4d00h19m
SWITCH#
```

Device S2

Display the routing table on device S2, you can see:

- ✧ The internal AS learned through S1 is the route of the 192.168.100.0/24 network segment learned by the OSPF domain;
- ✧ Self-configured static route 80.0.0.0/6 and default route 0.0.0.0/0
- ✧ Route 192.168.200.0/24 learned through RIP of S3

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.10.20.2 to network 0.0.0.0

S*        0.0.0.0/0 [1/0] via 10.10.20.2, gigabitEthernet0/2
C         10.10.1.0/24 is directly connected, gigabitEthernet0/1
C         10.10.20.0/24 is directly connected, gigabitEthernet0/2
S         80.0.0.0/6 [1/0] via 10.10.20.2, gigabitEthernet0/2
O         192.168.100.0/24 [110/2] via 10.10.1.1, gigabitEthernet0/1, 4d00h25m
R         192.168.200.0/24 [120/1] via 10.10.20.2, gigabitEthernet0/2,
4d00h26m
SWITCH#
```

Device S3

Display the routing table on device S3, you can see:

- ✧ The route of network segment 192.168.100.0/24 redistributed from OSPF learned through RIP of S2;

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.20.0/24 is directly connected, gigabitEthernet0/2
R          192.168.100.0/24 [120/1] via 10.10.20.1, gigabitEthernet0/2, 00:00:08
C          192.168.200.0/24 is directly connected, gigabitEthernet0/1

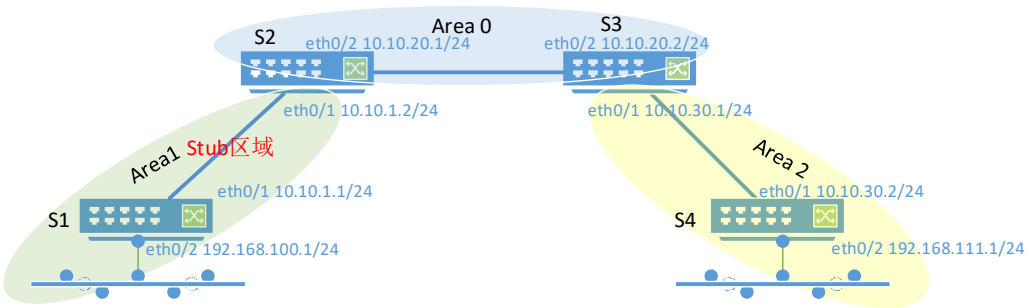
Gateway of last resort is not set
SWITCH#
```

15.3.2 OSPF StubRegional configuration

Requirements

- 4 devices are configured with 3 areas in an autonomous area; one of the areas is configured as a stub area to reduce the size of the routing table and reduce routing information transmission.
- The device runs the OSPF protocol;
- Each device can learn all routes in the autonomous domain;

Networking



Config. Case

For the interface IP and OSPF basic configuration, see the configuration example in Chapter 20.3.1 OSPF Basic Configuration. For the Stub domain related configuration of the area1 of S1 and S2.

- Device S1 configuration steps

Configure Area1 as a stub domain

```
S1(config-router)#area 1 stub
```

- Device S2 configuration steps

Configure Area1 as a stub domain

Configuring the no-summary parameter can prevent the ABR from sending network summary link advertisements to the stub domain (the configured stub domain is the Totally Stub domain, that is, the all-stub domain). This parameter can only be configured on ABR devices.

```
S1(config-router)#area 1 stub no-summary
```

- Results display

Device S1：

Display the routing table on device S1, and you can see that only one default route to the external domain is reserved on device S1.

```
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.10.1.2 to network 0.0.0.0

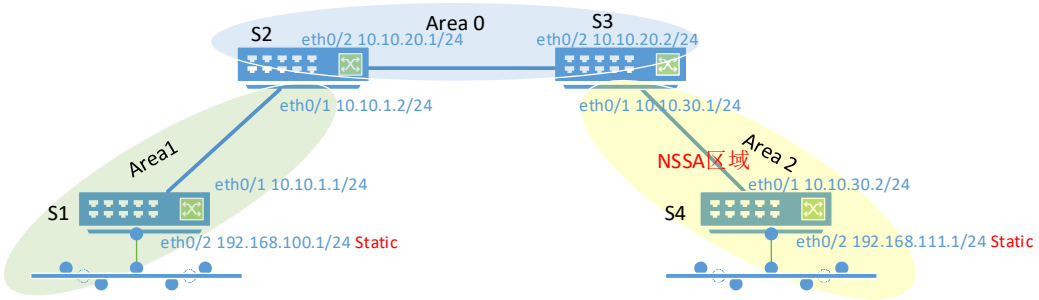
O*IA    0.0.0.0/0 [110/2] via 10.10.1.2, gigabitEthernet0/1, 00:18:33
C       10.10.1.0/24 is directly connected, gigabitEthernet0/1
C       192.168.100.0/24 is directly connected, gigabitEthernet0/2
S1#
```

15.3.2. OSPF NSSA Area Configuration

Requirements

- 4 devices are configured with 3 areas in an autonomous area; one of the areas is configured as an NSSA area to reduce the size of the routing table and reduce routing information transmission.
- The device runs the OSPF protocol;
- Each device can learn all routes in the autonomous domain;

Networking



Config,eg.

For the interface IP and OSPF basic configuration, see the configuration example in Chapter 20.3.1 OSPF Basic Configuration. Correspondingly, the static route redistribution of S1, and the NSSA domain related configuration of area2 of S3 and S4 are added.

- Device S1 configuration steps

Configure static routes

```
S1(config)#ip route 112.0.0.0/6 192.168.100.2
```

Configure static route redistribution

```
S1(config-router)#redistribute static
```

- Device S3 configuration steps

Configure Area2 as an NSSA domain Configuring the no-summary parameter can prevent the ABR from sending summary LSAs to the NSSA domain.

This parameter is only configured on the ABR device.

```
S1(config-router)#area 2 nssa no-summary
```

- Device S4 configuration steps

Configure static routes

```
S4(config)#ip route 80.0.0.0/6 192.168.111.2
```

Configure static route redistribution

```
S4(config-router)#redistribute static
```

Configure Area2 as an NSSA domain

```
S1(config-router)#area 2 nssa
```

- Results display

Before S3 and S4 configure area 2 as an NSSA domain:

Device S1：

The routing table displayed on device S1 is as follows. You can see that there are all routes advertised in the autonomous domain on device S1, including:

- ✧ The route to the 80.0.0.0/6 network segment, that is, the static route advertised by S4
- ✧ The route to the network segment 192.168.111.0/24, that is, the dynamic route advertised by S4

```
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
O IA       10.10.20.0/24 [110/2] via 10.10.1.2, gigabitEthernet0/1, 00:13:28
O IA       10.10.30.0/24 [110/3] via 10.10.1.2, gigabitEthernet0/1, 00:13:28
O E2       80.0.0.0/6 [110/20] via 10.10.1.2, gigabitEthernet0/1, 00:12:38
S          112.0.0.0/6 [1/0] via 192.168.100.2, gigabitEthernet0/2
C          192.168.100.0/24 is directly connected, gigabitEthernet0/2
O IA       192.168.111.0/24 [110/4] via 10.10.1.2, gigabitEthernet0/1, 00:13:28

Gateway of last resort is not set
S1#
```

Device S3：

The routing table displayed on device S3 is as follows. You can see that all routes advertised in the autonomous domain exist on the S3 device.

```
S3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
          * - candidate default

IP Route Table for VRF "default"
O IA       10.10.1.0/24 [110/2] via 10.10.20.1, gigabitEthernet0/2, 01:35:21
C           10.10.20.0/24 is directly connected, gigabitEthernet0/2
C           10.10.30.0/24 is directly connected, gigabitEthernet0/1
O E2       80.0.0.0/6 [110/20] via 10.10.30.2, gigabitEthernet0/1, 00:16:37
O E2       112.0.0.0/6 [110/20] via 10.10.20.1, gigabitEthernet0/2, 00:16:18
O IA       192.168.100.0/24 [110/3] via 10.10.20.1, gigabitEthernet0/2,
00:17:27
C           192.168.101.0/24 is directly connected, vlan100
O           192.168.111.0/24 [110/2] via 10.10.30.2, gigabitEthernet0/1,
01:51:26

Gateway of last resort is not set
S3#
```

Device S4：

The routing table displayed on device S4 is as follows. You can see that all routes advertised in the autonomous domain exist on the S4 device.

```
S4#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default

IP Route Table for VRF "default"
O IA       10.10.1.0/24 [110/3] via 10.10.30.1, gigabitEthernet0/1, 01:37:28
O IA       10.10.20.0/24 [110/2] via 10.10.30.1, gigabitEthernet0/1, 01:38:18
C           10.10.30.0/24 is directly connected, gigabitEthernet0/1
S           80.0.0.0/6 [1/0] via 192.168.111.2, gigabitEthernet0/2
O E2       112.0.0.0/6 [110/20] via 10.10.30.1, gigabitEthernet0/1, 00:18:25
O IA       192.168.100.0/24 [110/4] via 10.10.30.1, gigabitEthernet0/1,
00:19:33
C           192.168.111.0/24 is directly connected, gigabitEthernet0/2

Gateway of last resort is not set
S4#
```

After configuring area 2 as an NSSA domain on S3 and S4:

Device S1:

The routing table displayed on device S1 is as follows. You can see that there are all routes advertised in the autonomous domain on device S1, including:

- ✧ The route to the 80.0.0.0/6 network segment, that is, the static route advertised by S4
- ✧ The route to the network segment 192.168.111.0/24, that is, the dynamic route advertised by S4

```
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
O IA       10.10.20.0/24 [110/2] via 10.10.1.2, gigabitEthernet0/1, 00:05:28
O IA       10.10.30.0/24 [110/3] via 10.10.1.2, gigabitEthernet0/1, 00:05:28
O E2       80.0.0.0/6 [110/20] via 10.10.1.2, gigabitEthernet0/1, 00:01:18
S          112.0.0.0/6 [1/0] via 192.168.100.2, gigabitEthernet0/2
C          192.168.100.0/24 is directly connected, gigabitEthernet0/2
O IA       192.168.111.0/24 [110/4] via 10.10.1.2, gigabitEthernet0/1, 00:01:19

Gateway of last resort is not set
S1#
```

Device S3:

The routing table displayed on device S3 is as follows. You can see that all routes advertised in the autonomous domain exist on the S3 device, but the route 80.0.0.0/6 outside the autonomous domain imported by S4 has changed from E2 type to N2 type and is passed to other domains

```
S3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
```

```
O IA       10.10.1.0/24 [110/2] via 10.10.20.1, gigabitEthernet0/2, 00:07:46
C           10.10.20.0/24 is directly connected, gigabitEthernet0/2
C           10.10.30.0/24 is directly connected, gigabitEthernet0/1
O N2       80.0.0.0/6 [110/20] via 10.10.30.2, gigabitEthernet0/1, 00:03:27
O E2       112.0.0.0/6 [110/20] via 10.10.20.1, gigabitEthernet0/2, 00:04:12
O IA       192.168.100.0/24 [110/3] via 10.10.20.1, gigabitEthernet0/2,
00:04:13
C           192.168.101.0/24 is directly connected, vlan100
O           192.168.111.0/24 [110/2] via 10.10.30.2, gigabitEthernet0/1,
00:03:27

Gateway of last resort is not set
S3#
```

Device S4:

The routing table displayed on the device S4 is as follows. It can be seen that the routes on the S4 device have changed from all routes advertised in the autonomous domain to one less route 112.0.0.0/6 outside the autonomous domain imported by S1.

```
S4#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default

IP Route Table for VRF "default"
O IA       10.10.1.0/24 [110/3] via 10.10.30.1, gigabitEthernet0/1, 00:00:11
O IA       10.10.20.0/24 [110/2] via 10.10.30.1, gigabitEthernet0/1, 00:00:11
C           10.10.30.0/24 is directly connected, gigabitEthernet0/1
S           80.0.0.0/6 [1/0] via 192.168.111.2, gigabitEthernet0/2
O IA       192.168.100.0/24 [110/4] via 10.10.30.1, gigabitEthernet0/1, 00:00:11
C           192.168.111.0/24 is directly connected, gigabitEthernet0/2

Gateway of last resort is not set
S4#
```

After S3 and S4 configure area 2 as an NSSA domain and increase the no-summary parameter:

Device S4:

The routing table displayed on the device S4 is as follows. You can see that the routes on the S4 device have changed from all routes advertised in the autonomous domain to a default route.

```
S4#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.10.30.1 to network 0.0.0.0

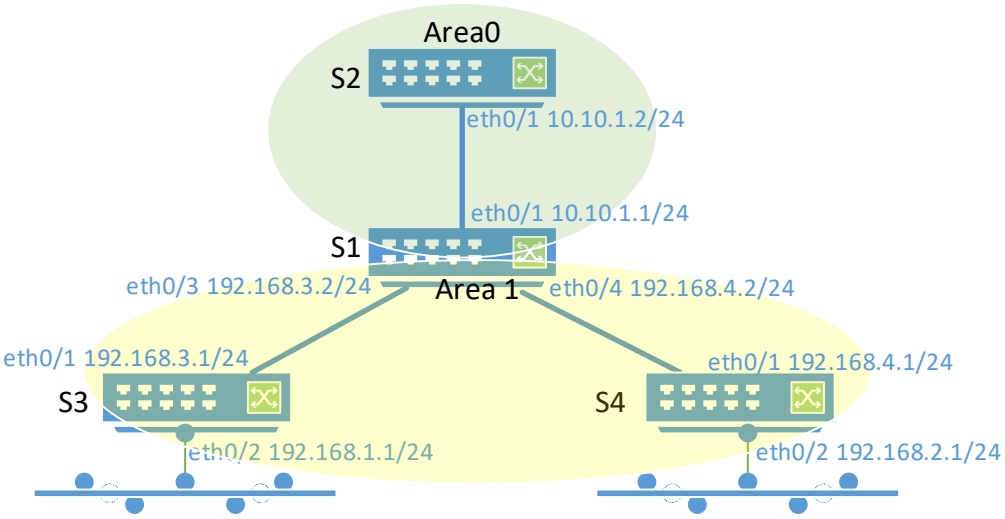
O*IA    0.0.0.0/0 [110/2] via 10.10.30.1, gigabitEthernet0/1, 00:08:06
C       10.10.30.0/24 is directly connected, gigabitEthernet0/1
S       80.0.0.0/6 [1/0] via 192.168.111.2, gigabitEthernet0/2
C       192.168.111.0/24 is directly connected, gigabitEthernet0/2
S4#
```

15.3.2. **OSPF route aggregation**

requirements

- 4 devices are configured with 3 areas in an autonomous area; one of the areas is configured as an NSSA area to reduce the size of the routing table and reduce routing information transmission.
- The device runs the OSPF protocol;
- Each device can learn all routes in the autonomous domain;

Networking



Config. Eg.

For the interface IP and basic OSPF configuration, see the configuration example in Chapter 20.3.1 Basic OSPF Configuration. For the route aggregation configuration of area1 that adds S1.

- Device S1 configuration steps

Configure route aggregation for Area1

Aggregate the four network segments 192.168.1.0/24 – 192.168.4.0/24 into one network segment 192.168.0.0/21.

```
S1(config-router)#area 1 range 192.168.0.0/21
```

- Results display

  Before the route aggregation command is configured on S1, the routing table of S2 has routes for the four network segments 192.168.1.0/24 – 192.168.4.0/24, as shown below

```
S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
O IA       192.168.1.0/24 [110/3] via 10.10.1.1, gigabitEthernet0/1, 00:00:02
O IA       192.168.2.0/24 [110/3] via 10.10.1.1, gigabitEthernet0/1, 00:00:02
O IA       192.168.3.0/24 [110/2] via 10.10.1.1, gigabitEthernet0/1, 00:00:02
O IA       192.168.4.0/24 [110/2] via 10.10.1.1, gigabitEthernet0/1, 00:00:02

Gateway of last resort is not set
S2#
```

After the route aggregation command is configured on S1, the routing table of S2 is as follows

```
S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
```

```
O IA       192.168.0.0/21 [110/3] via 10.10.1.1, gigabitEthernet0/1, 01:29:42

Gateway of last resort is not set
S2#
```

15.4. DISPLAY COMMAND

- Display routing information

```
S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default

IP Route Table for VRF "default"
C           10.10.1.0/24 is directly connected, gigabitEthernet0/1
O IA       192.168.0.0/21 [110/3] via 10.10.1.1, gigabitEthernet0/1, 01:30:09
O IA       192.168.1.0/24 [110/3] via 10.10.1.1, gigabitEthernet0/1, 00:00:02
O IA       192.168.2.0/24 [110/3] via 10.10.1.1, gigabitEthernet0/1, 00:00:02
O IA       192.168.3.0/24 [110/2] via 10.10.1.1, gigabitEthernet0/1, 00:00:02
O IA       192.168.4.0/24 [110/2] via 10.10.1.1, gigabitEthernet0/1, 00:00:02

Gateway of last resort is not set
S2#
```

- Only display OSPF routing information

```
S2#show ip route ospf
IP Route Table for VRF "default"
O IA       192.168.0.0/21 [110/3] via 10.10.1.1, gigabitEthernet0/1, 01:49:00
O IA       192.168.1.0/24 [110/3] via 10.10.1.1, gigabitEthernet0/1, 00:18:53
O IA       192.168.2.0/24 [110/3] via 10.10.1.1, gigabitEthernet0/1, 00:18:53
O IA       192.168.3.0/24 [110/2] via 10.10.1.1, gigabitEthernet0/1, 00:18:53
O IA       192.168.4.0/24 [110/2] via 10.10.1.1, gigabitEthernet0/1, 00:18:53

Gateway of last resort is not set
S2#
```

- Other OSPF information

Command	Function
show ip ospf process-id	Displays brief information about the process corresponding to OSPF
show ip ospf border-routers	Display OSPF border and border router information

show ip ospf database	Display OSPF database information
show ip ospf interface	Display OSPF interface-related information
show ip ospf neighbor	Display OSPF neighbor information

16. CONFIG.BGP

16.1. BGP OVERVIEW

BGP (Border Gateway Protocol) is an exterior gateway protocol (Exterior Gateway Protocol, EGP) that communicates between routing devices of different autonomous systems. Its main function is to exchange networks between different autonomous systems (Autonomous Systems, AS). reachable information, and eliminate routing loops through the protocol's own mechanism.

BGP uses the TCP protocol as the transmission protocol, and ensures the transmission reliability of BGP through the reliable transmission mechanism of the TCP protocol.

A router running the BGP protocol is called a BGP speaker, and the BGP speakers that establish a BGP session connection (BGP Session) are called peers (BGP peers).

There are two modes for establishing peers between BGP speakers: IBGP (Internal BGP) and EBGP (External BGP). IBGP refers to BGP connections established within the same AS, and EBGP refers to BGP connections established between different ASs.

In short, the functions of the two are as follows: EBGP is to complete the exchange of routing information between different ASs, and IBGP is to complete the transition of routing information within this AS.

16.2. CONFIG. COMMAND

16.2.1. **Create BGP process**

Command	SWITCH(config)#**router bgp** *as-number* SWITCH(config-router)# **bgp router-id** *router-id*
Description	Create a process and configure a unique ID.

16.2.2.BGP address family configuration

Command	SWITCH(config-router)#address-family ipv4 [unicast | multicast]
Description	The routing mode of BGP is in the IPv4 unicast address family. Commands configured by address family, configured in BGP routing mode, will act on the IPv4 unicast address family.

16.2.2. **BGP neighbors Config,**

BGP neighbors need to be manually configured, and both ends of the BGP session need to be configured as peer neighbors at the same time. Therefore, BGP neighbors are also called BGP peers.

- Configure peers

Command	SWITCH(config-router)# [**no**] **neighbor** *address* **remote-as** *as-number*
Description	address indicates the address of the BGP peer. as-number represents the as number in the range 1 – 4294967295.

- Configure the peer group

Command	SWITCH(config-router)# [**no**] **neighbor** *group-name* peer-group SWITCH(config-router)#[**no**]**neighbor address peer-group** *group-name* SWITCH(config-router)#**neighbor** *group-name* **remote-as** *as-number*
Description	group-name indicates the BGP peer group name. as-number indicates the as number in the range 1 - 4294967295.

16.2.3. Reflector Configuration

All BGP speakers in an AS need to establish full connections. Therefore, as the number of BGP speakers in the AS increases, the connections that need to be maintained between the speakers also increase accordingly, which will increase the resource consumption of the speakers. In order to reduce this consumption, you can use the BGP route reflector to design the network.

In the use of route reflectors, BGP speaker devices can be classified into clients and non-clients according to their types. A group is formed between a route reflector and its client (more than one). The client of the route reflector only establishes a connection with the reflector, no connection is established between the client and the client, and no connection is established between the client and the speaker outside the group. Based on the above principles, the BGP route reflector can reduce AS The number of connections in IBGP peers.

Configuring a router as a reflector is all about specifying which neighbors are clients to it.

The rules of route reflector for route learning are as follows:

- The routes learned by the client will be synchronized to other clients and other non-clients;
- Routes learned by non-clients through IBGP will be synchronized to other clients.
- Routes learned through EBGP Speaker will be synchronized to other clients and other non-clients;

If there are multiple route reflectors in a group, you need to configure a group ID for the group. If there is only one route reflector, this need not be configured. The group is identified by the router-id of the reflector.

- Configure the device as a route reflector and specify the client

Command	SWITCH(config-router)# [**no**] **neighbor** {**address** | *group-name* } **route-reflector-client**

Description	address indicates the peer IP address. group-name indicates the peer group address.

- Configure the route reflector group ID

Command	SWITCH(config-router)#**bgp cluster-id** *cluster-id*
Description	cluster-id indicates the cluster ID of the route reflector.

- Configure to cancel route reflection between clients

Command	SWITCH(config-router)#**no bgp client-to-client reflection**
Description	Cancel route reflection between clients.

16.2.3.AS Alliance Configuration

AS confederation can be used to reduce the number of connections to peers in homebrew systems (another approach is to configure route reflectors).

By configuring AS confederation, an autonomous system can be divided into multiple subsystems, and the subsystems can be merged into an confederation by setting the same confederation ID. For external autonomous systems, the confederation is an AS and a unified confederation AS number; for confederations Internally, BGP speakers are still connected according to complete IBGP peers, and BGP speakers between subsystems are still connected according to EBGP.

- Configure the AS alliance number

Command	SWITCH(config-router)#**bgp confederation identifier** *as-number*
Description	as-number is the Union number

- Configure other sub-ASs in the confederation

Command	SWITCH(config-router)#**bgp confederation peer** *as-number1 ..... as-numberN*
Description	as-number1 – asnumberN indicates the sub-as number that joins the alliance.

16.2.3. Route Aggregation Configuration

Command	SWITCH(config-router)#**aggregate-address** *address mask* [as-set] [summary-only]
Description	The address and mask parameters indicate the configured aggregate address. The as-set parameter indicates that if this parameter is configured, the AS path information of the paths in the aggregated address range will be retained.

	The summary-only parameter indicates that if this parameter is configured, only the aggregated paths will be advertised. The default is to advertise all path information before and after aggregation.

16.2.3. Route attenuation configuration

Frequent switching between valid and invalid routes will cause route flapping. This flapping may cause a chain reaction. Yes, the entire network is unstable. In order to solve such problems, the function of route attenuation is introduced.

The principle of the route damping function is that each time a route flap occurs, the corresponding route will increase the penalty value. When the cumulative penalty value exceeds the suppression threshold, the suppression will be triggered. The suppression time starts to count. When the count is equal to the half-life time, the penalty value becomes half of the original value and decreases in turn. When the penalty value is reduced to less than the restart value, the suppression of the route will be lifted and activated again.

Command	SWITCH(config-router)#**bgp dampening** [*half-life-time reuse-time suppress-time max-suppress-time*]
Description	The half-life-time parameter indicates the half-life, that is, the time when the penalty value is reduced to half, the unit is minutes, the range is 1-45, and the default value is 15. The reuse-time parameter indicates the restart value, that is, when the penalty value of the route is lower than this value, the route suppression is released. The range is 1-20000, the default is 750. The suppress-time parameter indicates the upper limit of suppression, that is, when the penalty value of a route is higher than this value, route suppression takes effect. The range is 1-20000, the default is 2000. max-suppress-time indicates the maximum time for route suppression, in minutes, ranging from 1 to 255. The default value is 4 times half-life-time.

Command	SWITCH#**show ip bgp dampening** {flap-statics | dampened-paths}
Description	The flap-statics parameter is used to view statistics about route flapping. The dampened-paths parameter is used to view suppressed statistics.

Command	SWITCH#**clear ip bgp dampening** {flap-statics [address [mask]] | dampened-paths [address [mask]]}
Description	The flap-statics parameter is used to clear the statistics of all route flaps. If the address and mask parameters are included, it is used to clear the statistics of the specified route. The dampened-paths parameter is used to clear the statistics of all suppressed routes. The suppressed routes are also contacted and suppressed. If the address and mask parameters are included, they are used to clear the statistics of the specified route.

16.2.3. Administrative Distance Configuration

The administrative distance is an attribute used to evaluate the reliability of the route source. The smaller the administrative distance, the higher the priority of the route.

Command	SWITCH(config-router)#**distance bgp** *external-distance internal-distance local-distance*
Description	The external-distance parameter indicates the administrative distance of routes learned from EBGP peers. The internal-distance parameter indicates the administrative distance of routes learned from IBGP peers. The local-distance parameter indicates the administrative distance learned from the peer, but it is considered that there are better routes that can be learned from the IGP, usually these routes are expressed through the network backdoor command.

If a route is configured as a backdoor route, if both IGP and EBGP learn the route, the IGP route will be used preferentially, but the route learned by the IGP will not be advertised.

Command	SWITCH(config-router)#**network** *address mask* **backdoor**
Description	The address and mask parameters indicate the network segment address. The backdoor parameter indicates that this route is a backdoor route.

16.2.3. Multipath Load Balancing Configuration

If there are multiple paths to a unified network segment, data can be forwarded in a balanced manner through these multiple paths, which is called multi-path load balancing. You can enable or disable this function by enabling/disabling the multi-path load balancing configuration. In BGP, EBGP routes can form multi-path load balancing with EBGP routes, but cannot form multi-path load balancing with IBGP routes. Similarly, IBPG cannot form multi-path load balancing with EBGP routes.

- EBGP multi-path load balancing

Command	SWITCH(config-router)#**maximum-paths ebgp** *number*
Description	number indicates the number of equivalent jumps supported, ranging from 1 to 32.

- IBGP multi-path load balancing

Command	SWITCH(config-router)#**maximum-paths ibgp** *number*
Description	number indicates the number of equivalent jumps supported, ranging from 1 to 32.

- EIBGP multi-path load balancing

Only one command can configure multi-path load balancing of EBGP and IBGP at the same time.

Command	SWITCH(config-router)#**maximum-paths eibgp** *number*
Description	number indicates the number of equivalent jumps supported, ranging from 1 to 32.

- AS-path loose comparison

By default, if two routes are to be combined into an equal-cost route to form multi-path load balancing, all attributes of the AS-path must be completely equal. If you want to reduce the above harsh conditions to form multi-path load balancing, you can achieve this by enabling AS-path loose comparison. AS-path loose comparison only needs to satisfy the condition that the AS-path length and the confederation AS-path length are equal respectively under the premise of the same route multi-path to achieve multi-path load balancing.

Command	SWITCH(config-router)#**bgp bestpath as-path multipath-relax**
Description	The command indicates to enable BGP AS-path loose comparison mode

16.2.4. Next-hop update trigger configuration

Command	SWITCH(config-router)#**bgp nexthop trigger enable**
Description	Next-hop update trigger enable configuration

Command	SWITCH(config-router)#**bgp nexthop trigger delay** *delay-time*
Description	Next update trigger time configuration

16.2.4. Route redistribution configuration

- Route injection

Command	SWITCH(config-router)# **redistribute** { connected | isis [area-tag] | ospf process-id | rip | static} [metric value] [metric-type {1 | 2}] [route-map map-name] [subnets] [tag value]
Description	This command is used to inject external routes (including static routes/routes of other routing protocols) into the BGP process.

- Default route injection

Command	SWITCH(config-router)#**default-informnation originate**
Description	Use this command to inject a default route into BGP, which is distributed over the protocol.

16.2.4. Protocol parameter configuration

- Configure the neighbor keepalive timer

Command	SWITCH(config-router)#**timer bgp** *keepalive holdtime*
Description	The keepalive parameter refers to the period for the peer to keep a valid connection, the unit is seconds, the range is 0-65535, and the default value is 60. During the keepalive period, the protocol will send keepalive packets to keep the connection. The holdtime parameter is the period for judging whether the peer is valid, the unit is seconds, the range is 0-65535, and the default value is 180. If the device does not receive the keepalive message from the peer within the holdtime, the peer connection is considered invalid.

When a BGP connection is established between BGP speakers, the holdtime will be negotiated, and the smaller holdtime will be selected as the effective configuration. The effective value of keepalive will be 1/3 of the effective holdtime value based on the negotiation after holdtime negotiation is completed, compared with the configured keepalive value, and the smaller value of the two is used as the effective configuration of keepalive.

You can also configure keepalive and holdtime values based on BGP peers (groups).

Command	SWITCH(config-router)#**neighbor** {address | group-name} *keepalive holdtime*
Description	adress indicates the address of the peer. group-name indicates the name of the peer group.

- Configure the neighbor reconnection timer

After the connection between the device and the peer fails, it needs to try to reconnect. You can configure the reconnection timer to specify the reconnection period.

Command	SWITCH(config-router)#**neighbor** {address | group-name} **timer connect** *connect-retry*
Description	adress indicates the address of the peer. group-name indicates the name of the peer group. connect-retry indicates the reconnection period, in seconds, ranging from 1 to 65535. The default value is 15 seconds.

- Configure the route advertisement timer

When a route change occurs locally, the device needs to advertise the updated route to peers (groups).

You can configure the route advertisement timer to set the advertisement frequency.

Command	SWITCH(config-router)#**neighbor** {address | group-name} **advertisemet-interval** *interval-time*
Description	adress indicates the address of the peer. group-name indicates the name of the peer group. interval-time indicates the minimum interval for sending routing updates, in seconds, ranging from 1 to 600. The default value is 5 seconds for IBGP peers and 30 seconds for EBGP peers.

The minimum time interval for sending locally originated routing updates can be configured.

Command	SWITCH(config-router)#**neighbor** {address | group-name} **as-origination-interval** *interval-time*
Description	adress indicates the address of the peer. group-name indicates the name of the peer group. interval-time indicates the minimum interval for sending routing updates, in seconds, ranging from 1 to 600. The default value is 1 second.

16.3. CONFIG.CASE

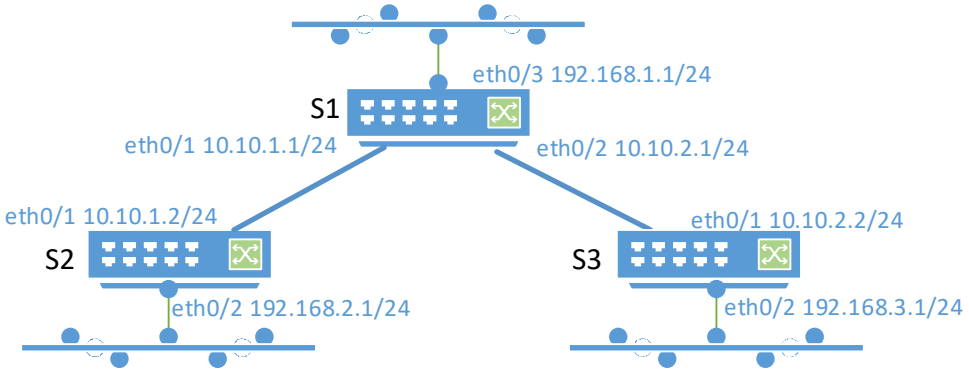
16.3.1. **BGP Basic Config.**

16.3.1.1. Creating peers

Requirements

- 3 devices exchange routes using BGP protocol;
- S1 and S2 establish IBGP neighbors, and S1 and S3 establish EBGP neighbors

Networking



Config.Eg.

- Device S1 configuration steps

Create BGP process

```
S1#configure terminal
S1(config)#router bgp 100
S1(config-router)#neighbor 10.10.1.2 remote-as 100
S1(config-router)#neighbor 10.10.2.2 remote-as 200
S1(config-router)#network 192.168.1.0/24
```

Configure the ip address of port gigabitEthernet0/1

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/1
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.1.1/24
```

Configure the ip address of port gigabitEthernet0/2

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/2
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.2.1/24
```

Configure the ip address of port gigabitEthernet0/3

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/3
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.1.1/24
```

- Device S2 configuration steps

Create BGP process

```
S2#configure terminal
S2(config)#router bgp 100
S2(config-router)#neighbor 10.10.1.1 remote-as 100
```

```
S2(config-router)#network 192.168.2.0/24
```

Configure the ip address of port gigabitEthernet0/1

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/1
S2(config-if)#no switchport
S2(config-if)#ip address 10.10.1.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/2
S2(config-if)#no switchport
S2(config-if)#ip address 192.168.2.1/24
```

- Device S3 configuration steps

Create BGP Process

```
S3#configure terminal
S3(config)#router bgp 200
S3(config-router)#neighbor 10.10.2.1 remote-as 100
S3(config-router)#network 192.168.3.0/24
```

Configure the ip address of port gigabitEthernet0/1

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/1
S3(config-if)#no switchport
S3(config-if)#ip address 10.10.2.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/2
S3(config-if)#no switchport
S3(config-if)#ip address 192.168.3.1/24
```

- Results display

Device S1：

Display bgp neighbor information and routing table on device S1

```
S1#show ip bgp neighbors
BGP neighbor is 10.10.1.2, remote AS 100, local AS 100, internal link
  BGP version 4, remote router ID 192.168.2.1
  BGP state = Established, up for 00:07:20
  Last read 00:07:20, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
```

```
      Address family IPv4 Unicast: advertised and received
    Received 12 messages, 0 notifications, 0 in queue
    Sent 12 messages, 0 notifications, 0 in queue
    Route refresh request: received 0, sent 0
    Minimum time between advertisement runs is 0 seconds

  For address family: IPv4 Unicast
    BGP table version 3, neighbor version 3
    Index 1, Offset 0, Mask 0x2
    Community attribute sent to this neighbor (both)
    1 accepted prefixes
    4 announced prefixes

  Connections established 1; dropped 0
Local host: 10.10.1.1, Local port: 179
Foreign host: 10.10.1.2, Foreign port: 51608
Nexthop: 10.10.1.1

BGP neighbor is 10.10.2.2, remote AS 200, local AS 100, external link
    BGP version 4, remote router ID 192.168.3.1
    BGP state = Established, up for 00:07:20
    Last read 00:07:19, hold time is 180, keepalive interval is 60 seconds
    Neighbor capabilities:
      Route refresh: advertised and received (old and new)
      Four-octets ASN Capability: advertised and received
      Address family IPv4 Unicast: advertised and received
    Received 12 messages, 0 notifications, 0 in queue
    Sent 12 messages, 0 notifications, 0 in queue
    Route refresh request: received 0, sent 0
    Minimum time between advertisement runs is 30 seconds

  For address family: IPv4 Unicast
    BGP table version 3, neighbor version 3
    Index 2, Offset 0, Mask 0x4
    Community attribute sent to this neighbor (both)
    1 accepted prefixes
    4 announced prefixes

  Connections established 1; dropped 0
Local host: 10.10.2.1, Local port: 58948
Foreign host: 10.10.2.2, Foreign port: 179
Nexthop: 10.10.2.1
```

```
Last Reset:              , due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

S1#
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
C          10.10.2.0/24 is directly connected, gigabitEthernet0/2
C          192.168.1.0/24 is directly connected, gigabitEthernet0/3
B          192.168.2.0/24 [200/0] via 10.10.1.2, gigabitEthernet0/1, 00:07:24
B          192.168.3.0/24 [20/0] via 10.10.2.2, gigabitEthernet0/2, 00:07:24
C          192.168.101.0/24 is directly connected, gigabitEthernet0/24

Gateway of last resort is not set
S1#
```

Device S2:

Display bgp neighbor information and routing table on device S2

```
S2#show ip bgp neighbors
BGP neighbor is 10.10.1.1, remote AS 100, local AS 100, internal link
  BGP version 4, remote router ID 10.10.1.1
  BGP state = Established, up for 00:08:33
  Last read 00:08:32, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 115 messages, 0 notifications, 0 in queue
  Sent 108 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 0 seconds

 For address family: IPv4 Unicast
  BGP table version 10, neighbor version 10
  Index 1, Offset 0, Mask 0x2
```

```
  Community attribute sent to this neighbor (both)
  4 accepted prefixes
  1 announced prefixes

 Connections established 4; dropped 3
Local host: 10.10.1.2, Local port: 51608
Foreign host: 10.10.1.1, Foreign port: 179
Nexthop: 10.10.1.2

S2#
S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
B          192.168.1.0/24 [200/0] via 10.10.1.1, gigabitEthernet0/1, 00:08:35
C          192.168.2.0/24 is directly connected, gigabitEthernet0/2

Gateway of last resort is not set
S2#
```

Device S3：

Display bgp neighbor information and routing table on device S3

```
S3#show ip bgp neighbors
BGP neighbor is 10.10.2.1, remote AS 100, local AS 200, external link
  BGP version 4, remote router ID 10.10.1.1
  BGP state = Established, up for 00:09:09
  Last read 00:09:08, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 125 messages, 0 notifications, 0 in queue
  Sent 114 messages, 3 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
```

```
  For address family: IPv4 Unicast
    BGP table version 5, neighbor version 4
    Index 1, Offset 0, Mask 0x2
    Community attribute sent to this neighbor (both)
    4 accepted prefixes
    1 announced prefixes

  Connections established 4; dropped 3
Local host: 10.10.2.2, Local port: 179
Foreign host: 10.10.2.1, Foreign port: 58948
Nexthop: 10.10.2.2
Last Reset: 00:10:40, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

S3#
S3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
           * - candidate default

IP Route Table for VRF "default"
C          10.10.2.0/24 is directly connected, gigabitEthernet0/1
B          192.168.1.0/24 [20/0] via 10.10.2.1, gigabitEthernet0/1, 00:09:11
B          192.168.2.0/24 [20/0] via 10.10.2.1, gigabitEthernet0/1, 00:09:11
C          192.168.3.0/24 is directly connected, vlan200

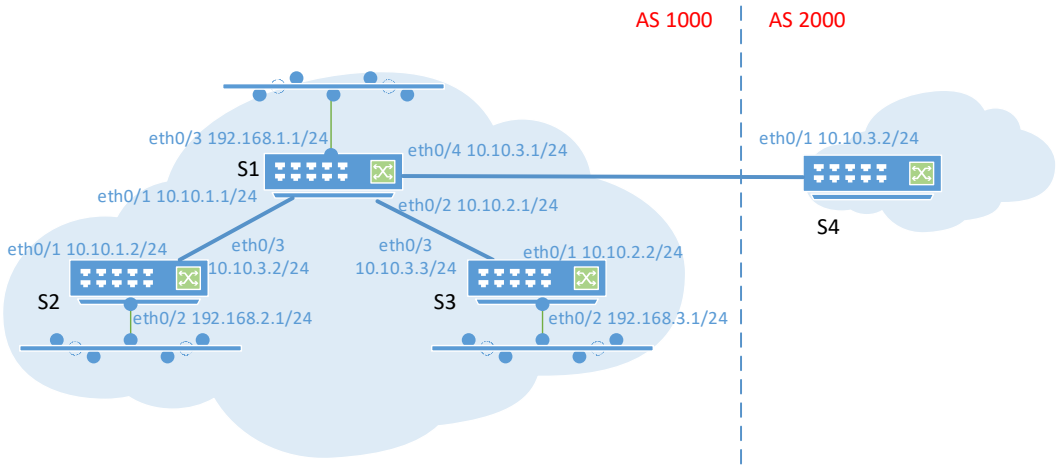
Gateway of last resort is not set
S3#
```

16.3.1.1. Create a peer group

Requirements

- S1, S2, S3, S4, 4 devices use BGP protocol to exchange routes;
- S1, S2, S3 establish IBGP neighbors; S1 and S4 establish EBGP neighbors;
- Create a peer group on S3

Networking



Config.Eg.

- Device S1 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/1
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.1.1/24
```

Configure the ip address of port gigabitEthernet0/2

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/2
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.2.1/24
```

Configure the ip address of port gigabitEthernet0/3

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/3
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.1.1/24
```

Configure the ip address of port gigabitEthernet0/4

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/4
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.3.1/24
```

Create a BGP process and a peer group, and name the peer group peer-group-test

```
S1#configure terminal
S1(config)#router bgp 1000
S1(config-router)#neighbor peer-group-test peer-group
S1(config-router)#neighbor peer-group-test remote-as 1000
S1(config-router)#neighbor peer-group-test next-hop-self
S1(config-router)#neighbor 10.10.1.2 peer-group peer-group-test
S1(config-router)#neighbor 10.10.2.2 peer-group peer-group-test
S1(config-router)#neighbor 10.10.3.2 remote-as 2000
S1(config-router)#network 192.168.1.0/24
S1(config-router)#network 10.10.1.0/24
S1(config-router)#network 10.10.2.0/24
S1(config-router)#network 10.10.3.0/24
```

- Device S2 configuration steps

Create BGP process

```
S2#configure terminal
S2(config)#router bgp 1000
S2(config-router)#neighbor 10.10.1.1 remote-as 1000
S2(config-router)#network 192.168.2.0/24
```

Configure the ip address of port gigabitEthernet0/1

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/1
S2(config-if)#no switchport
S2(config-if)#ip address 10.10.1.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/2
S2(config-if)#no switchport
S2(config-if)#ip address 192.168.2.1/24
```

- Device S3 configuration steps

Create BGP process

```
S3#configure terminal
S3(config)#router bgp 200
```

```
S3(config-router)#neighbor 10.10.2.1 remote-as 100
S3(config-router)#network 192.168.3.0/24
```

Configure the ip address of port gigabitEthernet0/1

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/1
S3(config-if)#no switchport
S3(config-if)#ip address 10.10.2.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/2
S3(config-if)#no switchport
S3(config-if)#ip address 192.168.3.1/24
```

- Device S4 configuration steps

Create BGP process

```
S4#configure terminal
S4(config)#router bgp 2000
S4(config-router)#neighbor 10.10.3.1 remote-as 1000
S4(config-router)#network 192.168.4.0/24
```

Configure the ip address of port gigabitEthernet0/1

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/1
S4(config-if)#no switchport
S4(config-if)#ip address 10.10.3.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/2
S4(config-if)#no switchport
S4(config-if)#ip address 192.168.4.1/24
```

- Results display

Device S1：

Display bgp neighbor information and routing table on device S1

```
S1#show ip bgp neighbors
BGP neighbor is 10.10.1.2, remote AS 1000, local AS 1000, internal link
  Member of peer-group peer-group-test for session parameters
    BGP version 4, remote router ID 10.10.1.2
    BGP state = Established, up for 00:05:53
    Last read 00:05:52, hold time is 180, keepalive interval is 60 seconds
    Neighbor capabilities:
      Route refresh: advertised and received (old and new)
      Four-octets ASN Capability: advertised and received
```

```
      Address family IPv4 Unicast: advertised and received
    Received 10 messages, 0 notifications, 0 in queue
    Sent 10 messages, 0 notifications, 0 in queue
    Route refresh request: received 0, sent 0
    Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
    BGP table version 4, neighbor version 4
    Index 1, Offset 0, Mask 0x2
    peer-group-test peer-group member
    NEXT_HOP is always this router
    Community attribute sent to this neighbor (both)
    1 accepted prefixes
    5 announced prefixes

  Connections established 1; dropped 0
Local host: 10.10.1.1, Local port: 43269
Foreign host: 10.10.1.2, Foreign port: 179
Nexthop: 10.10.1.1

BGP neighbor is 10.10.2.2, remote AS 1000, local AS 1000, internal link
  Member of peer-group peer-group-test for session parameters
    BGP version 4, remote router ID 192.168.3.1
    BGP state = Established, up for 00:05:51
    Last read 00:05:50, hold time is 180, keepalive interval is 60 seconds
    Neighbor capabilities:
      Route refresh: advertised and received (old and new)
      Four-octets ASN Capability: advertised and received
      Address family IPv4 Unicast: advertised and received
    Received 10 messages, 0 notifications, 0 in queue
    Sent 11 messages, 0 notifications, 0 in queue
    Route refresh request: received 0, sent 0
    Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
    BGP table version 4, neighbor version 4
    Index 2, Offset 0, Mask 0x4
    peer-group-test peer-group member
    NEXT_HOP is always this router
    Community attribute sent to this neighbor (both)
    1 accepted prefixes
    5 announced prefixes
```

```
  Connections established 1; dropped 0
Local host: 10.10.2.1, Local port: 179
Foreign host: 10.10.2.2, Foreign port: 41039
Nexthop: 10.10.2.1

BGP neighbor is 10.10.3.2, remote AS 2000, local AS 1000, external link
   BGP version 4, remote router ID 192.168.4.1
   BGP state = Established, up for 00:05:10
   Last read 00:05:09, hold time is 180, keepalive interval is 60 seconds
   Neighbor capabilities:
      Route refresh: advertised and received (old and new)
      Four-octets ASN Capability: advertised and received
      Address family IPv4 Unicast: advertised and received
   Received 10 messages, 0 notifications, 0 in queue
   Sent 9 messages, 0 notifications, 0 in queue
   Route refresh request: received 0, sent 0
   Minimum time between advertisement runs is 30 seconds

  For address family: IPv4 Unicast
   BGP table version 4, neighbor version 3
   Index 3, Offset 0, Mask 0x8
   Community attribute sent to this neighbor (both)
   1 accepted prefixes
   6 announced prefixes

  Connections established 1; dropped 0
Local host: 10.10.3.1, Local port: 179
Foreign host: 10.10.3.2, Foreign port: 57299
Nexthop: 10.10.3.1
Last Reset:              , due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

S1#
S1#
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default
```

```
IP Route Table for VRF "default"
C        10.10.1.0/24 is directly connected, gigabitEthernet0/1
C        10.10.2.0/24 is directly connected, gigabitEthernet0/2
C        10.10.3.0/24 is directly connected, gigabitEthernet0/4
C        192.168.1.0/24 is directly connected, gigabitEthernet0/3
B        192.168.2.0/24 [200/0] via 10.10.1.2, gigabitEthernet0/1, 00:05:56
B        192.168.3.0/24 [200/0] via 10.10.2.2, gigabitEthernet0/2, 00:05:54
B        192.168.4.0/24 [20/0] via 10.10.3.2, gigabitEthernet0/4, 00:05:13

Gateway of last resort is not set
S1#
```

Device S2:

Display bgp neighbor information and routing table on device S2

```
S2#show ip bgp neighbors
BGP neighbor is 10.10.1.1, remote AS 1000, local AS 1000, internal link
  BGP version 4, remote router ID 10.10.1.1
  BGP state = Established, up for 00:06:47
  Last read 00:06:02, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 14 messages, 0 notifications, 0 in queue
  Sent 10 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  5 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.1.2, Local port: 179
Foreign host: 10.10.1.1, Foreign port: 43269
Nexthop: 10.10.1.2

S2#
```

```
S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
B          10.10.2.0/24 [200/0] via 10.10.1.1, gigabitEthernet0/1, 00:06:50
B          10.10.3.0/24 [200/0] via 10.10.1.1, gigabitEthernet0/1, 00:06:37
B          192.168.1.0/24 [200/0] via 10.10.1.1, gigabitEthernet0/1, 00:06:50
C          192.168.2.0/24 is directly connected, gigabitEthernet0/2
B          192.168.4.0/24 [200/0] via 10.10.1.1, gigabitEthernet0/1, 00:06:06

Gateway of last resort is not set
S2#
```

Device S3：

Display bgp neighbor information and routing table on device S3

```
S3#show ip bgp neighbors
BGP neighbor is 10.10.2.1, remote AS 1000, local AS 1000, internal link
  BGP version 4, remote router ID 10.10.1.1
  BGP state = Established, up for 00:10:10
  Last read 00:09:27, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 19 messages, 0 notifications, 0 in queue
  Sent 15 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  5 accepted prefixes
  1 announced prefixes
```

```
  Connections established 1; dropped 0
Local host: 10.10.2.2, Local port: 41039
Foreign host: 10.10.2.1, Foreign port: 179
Nexthop: 10.10.2.2

S3#
S3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
B          10.10.1.0/24 [200/0] via 10.10.2.1, gigabitEthernet0/1, 00:10:11
C          10.10.2.0/24 is directly connected, gigabitEthernet0/1
B          10.10.3.0/24 [200/0] via 10.10.2.1, gigabitEthernet0/1, 00:10:00
B          192.168.1.0/24 [200/0] via 10.10.2.1, gigabitEthernet0/1, 00:10:11
C          192.168.3.0/24 is directly connected, vlan200
B          192.168.4.0/24 [200/0] via 10.10.2.1, gigabitEthernet0/1, 00:09:29

Gateway of last resort is not set
S3#
```

Device S4：

Display bgp neighbor information and routing table on device S4

```
S4#show ip bgp neighbors
BGP neighbor is 10.10.3.1, remote AS 1000, local AS 2000, external link
  BGP version 4, remote router ID 10.10.1.1
  BGP state = Established, up for 00:10:14
  Last read 00:10:13, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 17 messages, 0 notifications, 0 in queue
  Sent 15 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
```

```
  BGP table version 2, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  6 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.3.2, Local port: 57299
Foreign host: 10.10.3.1, Foreign port: 179
Nexthop: 10.10.3.2
Last Reset:              , due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

S4#
S4#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
B          10.10.1.0/24 [20/0] via 10.10.3.1, gigabitEthernet0/1, 00:10:18
B          10.10.2.0/24 [20/0] via 10.10.3.1, gigabitEthernet0/1, 00:10:18
C          10.10.3.0/24 is directly connected, gigabitEthernet0/1
B          192.168.1.0/24 [20/0] via 10.10.3.1, gigabitEthernet0/1, 00:10:18
B          192.168.2.0/24 [20/0] via 10.10.3.1, gigabitEthernet0/1, 00:10:18
B          192.168.3.0/24 [20/0] via 10.10.3.1, gigabitEthernet0/1, 00:10:18
C          192.168.4.0/24 is directly connected, gigabitEthernet0/2

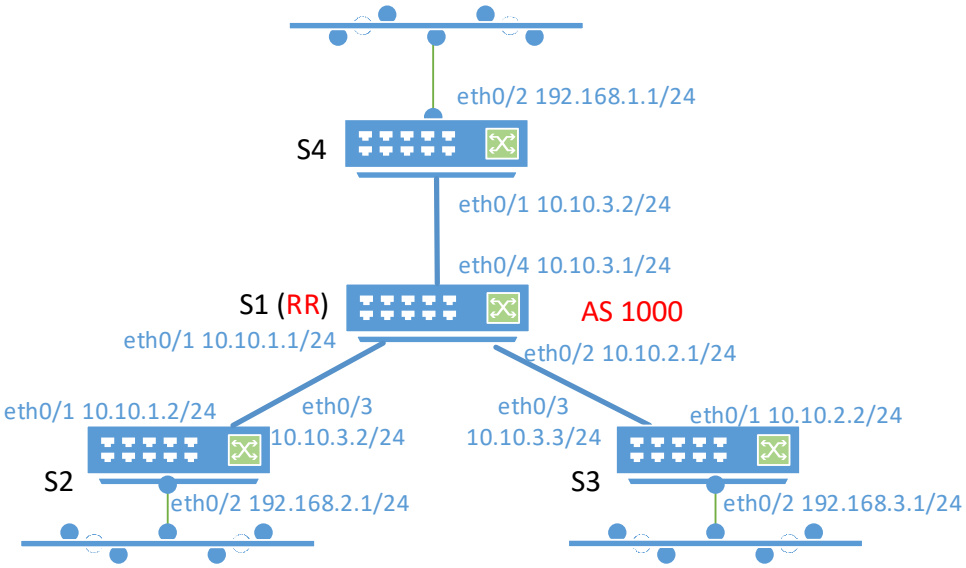
Gateway of last resort is not set
S4#
```

16.3.2. Route Reflector Configuration

Requirements

- 4 devices exchange routes using BGP protocol;
- S1 acts as a route reflector, and S2, S3, and S4 act as clients;

Networking



Config.Eg.

- Device S1 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/1
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.1.1/24
```

Configure the ip address of port gigabitEthernet0/2

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/2
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.2.1/24
```

Configure the ip address of port gigabitEthernet0/4

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/4
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.3.1/24
```

Create BGP process and reflector and client

```
S1#configure terminal
S1(config)#router bgp 1000
S1(config-router)#neighbor 10.10.1.2 remote-as 1000
S1(config-router)#neighbor 10.10.1.2 route-reflector-client
S1(config-router)#neighbor 10.10.2.2 remote-as 1000
S1(config-router)#neighbor 10.10.2.2 route-reflector-client
```

```
S1(config-router)#neighbor 10.10.3.2 remote-as 1000
S1(config-router)#neighbor 10.10.3.2 route-reflector-client
S1(config-router)#network 10.10.1.0/24
S1(config-router)#network 10.10.2.0/24
S1(config-router)#network 10.10.3.0/24
```

- Device S2 configuration steps

Create BGP process

```
S2#configure terminal
S2(config)#router bgp 100
S2(config-router)#neighbor 10.10.1.1 remote-as 100
S2(config-router)#network 192.168.2.0/24
```

Configure the ip address of port gigabitEthernet0/1

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/1
S2(config-if)#no switchport
S2(config-if)#ip address 10.10.1.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/2
S2(config-if)#no switchport
S2(config-if)#ip address 192.168.2.1/24
```

- Device S3 configuration steps

Create BGP Process

```
S3#configure terminal
S3(config)#router bgp 200
S3(config-router)#neighbor 10.10.2.1 remote-as 100
S3(config-router)#network 192.168.3.0/24
```

Configure the ip address of port gigabitEthernet0/1

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/1
S3(config-if)#no switchport
S3(config-if)#ip address 10.10.2.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/2
S3(config-if)#no switchport
S3(config-if)#ip address 192.168.3.1/24
```

- Device S4 configuration steps

Create BGP process

```
S4#configure terminal
S4(config)#router bgp 1000
S4(config-router)#neighbor 10.10.3.1 remote-as 1000
S4(config-router)#network 192.168.4.0/24
```

Configure the ip address of port gigabitEthernet0/1

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/1
S4(config-if)#no switchport
S4(config-if)#ip address 10.10.3.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/2
S4(config-if)#no switchport
S4(config-if)#ip address 192.168.4.1/24
```

- Results display

Device S1：

Display bgp neighbor information and routing table on device S1

```
S1#show ip bgp neighbors
BGP neighbor is 10.10.1.2, remote AS 1000, local AS 1000, internal link
   BGP version 4, remote router ID 10.10.1.2
   BGP state = Established, up for 00:06:08
   Last read 00:06:07, hold time is 180, keepalive interval is 60 seconds
   Neighbor capabilities:
      Route refresh: advertised and received (old and new)
      Four-octets ASN Capability: advertised and received
      Address family IPv4 Unicast: advertised and received
   Received 11 messages, 0 notifications, 0 in queue
   Sent 11 messages, 0 notifications, 0 in queue
   Route refresh request: received 0, sent 0
   Minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
   BGP table version 3, neighbor version 3
   Index 1, Offset 0, Mask 0x2
   Route-Reflector Client
   NEXT_HOP is always this router
   Community attribute sent to this neighbor (both)
   1 accepted prefixes
   5 announced prefixes

 Connections established 1; dropped 0
```

```
Local host: 10.10.1.1, Local port: 46298
Foreign host: 10.10.1.2, Foreign port: 179
Nexthop: 10.10.1.1
Last Reset:              , due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 10.10.2.2, remote AS 1000, local AS 1000, internal link
   BGP version 4, remote router ID 192.168.3.1
   BGP state = Established, up for 00:06:13
   Last read 00:06:12, hold time is 180, keepalive interval is 60 seconds
   Neighbor capabilities:
      Route refresh: advertised and received (old and new)
      Four-octets ASN Capability: advertised and received
      Address family IPv4 Unicast: advertised and received
   Received 11 messages, 0 notifications, 0 in queue
   Sent 12 messages, 0 notifications, 0 in queue
   Route refresh request: received 0, sent 0
   Minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
   BGP table version 3, neighbor version 3
   Index 2, Offset 0, Mask 0x4
   Route-Reflector Client
   NEXT_HOP is always this router
   Community attribute sent to this neighbor (both)
   1 accepted prefixes
   5 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.2.1, Local port: 179
Foreign host: 10.10.2.2, Foreign port: 48706
Nexthop: 10.10.2.1
Last Reset:              , due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 10.10.3.2, remote AS 1000, local AS 1000, internal link
   BGP version 4, remote router ID 192.168.4.1
   BGP state = Established, up for 00:05:58
   Last read 00:05:57, hold time is 180, keepalive interval is 60 seconds
   Neighbor capabilities:
      Route refresh: advertised and received (old and new)
      Four-octets ASN Capability: advertised and received
```

```
      Address family IPv4 Unicast: advertised and received
    Received 11 messages, 0 notifications, 0 in queue
    Sent 11 messages, 0 notifications, 0 in queue
    Route refresh request: received 0, sent 0
    Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
    BGP table version 3, neighbor version 2
    Index 3, Offset 0, Mask 0x8
    Route-Reflector Client
    NEXT_HOP is always this router
    Community attribute sent to this neighbor (both)
    1 accepted prefixes
    5 announced prefixes

  Connections established 1; dropped 0
Local host: 10.10.3.1, Local port: 179
Foreign host: 10.10.3.2, Foreign port: 42775
Nexthop: 10.10.3.1
Last Reset:              , due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

S1#
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
           * - candidate default

IP Route Table for VRF "default"
C           10.10.1.0/24 is directly connected, gigabitEthernet0/1
C           10.10.2.0/24 is directly connected, gigabitEthernet0/2
C           10.10.3.0/24 is directly connected, gigabitEthernet0/4
C           192.168.1.0/24 is directly connected, gigabitEthernet0/3
B           192.168.2.0/24 [200/0] via 10.10.1.2, gigabitEthernet0/1, 00:06:09
B           192.168.3.0/24 [200/0] via 10.10.2.2, gigabitEthernet0/2, 00:06:14
B           192.168.4.0/24 [200/0] via 10.10.3.2, gigabitEthernet0/4, 00:05:59

Gateway of last resort is not set
S1#
```

Device S2：

Display bgp neighbor information and routing table on device S2

```
S2#show ip bgp neighbors
BGP neighbor is 10.10.1.1, remote AS 1000, local AS 1000, internal link
   BGP version 4, remote router ID 192.168.1.1
   BGP state = Established, up for 00:03:00
   Last read 00:02:49, hold time is 180, keepalive interval is 60 seconds
   Neighbor capabilities:
      Route refresh: advertised and received (old and new)
      Four-octets ASN Capability: advertised and received
      Address family IPv4 Unicast: advertised and received
   Received 11 messages, 0 notifications, 0 in queue
   Sent 6 messages, 0 notifications, 0 in queue
   Route refresh request: received 0, sent 0
   Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
   BGP table version 2, neighbor version 1
   Index 1, Offset 0, Mask 0x2
   Community attribute sent to this neighbor (both)
   5 accepted prefixes
   1 announced prefixes

  Connections established 1; dropped 0
Local host: 10.10.1.2, Local port: 179
Foreign host: 10.10.1.1, Foreign port: 46298
Nexthop: 10.10.1.2

S2#
S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
B          10.10.2.0/24 [200/0] via 10.10.1.1, gigabitEthernet0/1, 00:03:03
B          10.10.3.0/24 [200/0] via 10.10.1.1, gigabitEthernet0/1, 00:03:03
```

```
C          192.168.2.0/24 is directly connected, gigabitEthernet0/2
B          192.168.3.0/24 [200/0] via 10.10.2.2 (recursive via 10.10.1.1 ),
00:02:57
B          192.168.4.0/24 [200/0] via 10.10.3.2 (recursive via 10.10.1.1 ),
00:02:53

Gateway of last resort is not set
S2#
```

Device S3：

Display bgp neighbor information and routing table on device S3

```
S3#show ip bgp neighbors
BGP neighbor is 10.10.2.1, remote AS 1000, local AS 1000, internal link
   BGP version 4, remote router ID 192.168.1.1
   BGP state = Established, up for 00:03:50
   Last read 00:03:34, hold time is 180, keepalive interval is 60 seconds
   Neighbor capabilities:
      Route refresh: advertised and received (old and new)
      Four-octets ASN Capability: advertised and received
      Address family IPv4 Unicast: advertised and received
   Received 12 messages, 0 notifications, 0 in queue
   Sent 7 messages, 0 notifications, 0 in queue
   Route refresh request: received 0, sent 0
   Minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
   BGP table version 2, neighbor version 1
   Index 1, Offset 0, Mask 0x2
   Community attribute sent to this neighbor (both)
   5 accepted prefixes
   1 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.2.2, Local port: 48706
Foreign host: 10.10.2.1, Foreign port: 179
Nexthop: 10.10.2.2

S3#
S3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default

IP Route Table for VRF "default"
B           10.10.1.0/24 [200/0] via 10.10.2.1, gigabitEthernet0/1, 00:03:53
C           10.10.2.0/24 is directly connected, gigabitEthernet0/1
B           10.10.3.0/24 [200/0] via 10.10.2.1, gigabitEthernet0/1, 00:03:53
B           192.168.2.0/24 [200/0] via 10.10.1.2 (recursive via 10.10.2.1 ),
00:03:47
C           192.168.3.0/24 is directly connected, vlan200
B           192.168.4.0/24 [200/0] via 10.10.3.2 (recursive via 10.10.2.1 ),
00:03:38

Gateway of last resort is not set
S3#
```

Device S4：

Display bgp neighbor information and routing table on device S4

```
S4#show ip bgp neighbors
BGP neighbor is 10.10.3.1, remote AS 1000, local AS 1000, internal link
  BGP version 4, remote router ID 192.168.1.1
  BGP state = Established, up for 00:04:14
  Last read 00:04:13, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 12 messages, 0 notifications, 0 in queue
  Sent 7 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  5 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.3.2, Local port: 42775
```

```
Foreign host: 10.10.3.1, Foreign port: 179
Nexthop: 10.10.3.2

S4#
S4#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
B          10.10.1.0/24 [200/0] via 10.10.3.1, gigabitEthernet0/1, 00:04:19
B          10.10.2.0/24 [200/0] via 10.10.3.1, gigabitEthernet0/1, 00:04:19
C          10.10.3.0/24 is directly connected, gigabitEthernet0/1
B          192.168.2.0/24 [200/0] via 10.10.1.2 (recursive via 10.10.3.1 ),
00:04:13
B          192.168.3.0/24 [200/0] via 10.10.2.2 (recursive via 10.10.3.1 ),
00:04:13
C          192.168.4.0/24 is directly connected, gigabitEthernet0/2

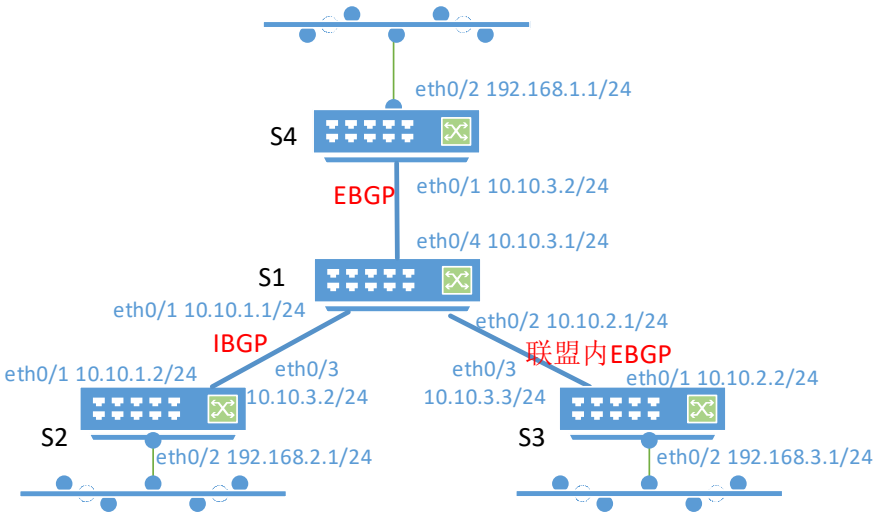
Gateway of last resort is not set
S4#
```

16.3.2.AS Alliance Configuration

Requirements

- 4 devices exchange routes using BGP protocol;
- S1, S2, and S3 are in the same confederation. S1 and S2 establish IBGP neighbors, and S1 and S3 establish EBGP neighbors;
- S4 establishes an EBGP neighbor relationship with the alliance where S1 is located;

Networking



CONFIG.Eg.

- Device S1 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/1
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.1.1/24
```

Configure the ip address of port gigabitEthernet0/2

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/2
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.2.1/24
```

Configure the ip address of port gigabitEthernet0/4

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/4
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.3.1/24
```

Create BGP process and configure alliance

The AS number is 1000, the alliance number is 111, the AS number of the EBGP within the alliance is 2000, and the AS number of the EBGP outside the alliance is 222

```
S1#configure terminal
S1(config)#router bgp 1000
S1(config-router)#bgp confederation identifier 111
S1(config-router)#bgp confederation peers 2000
S1(config-router)#neighbor 10.10.1.2 remote-as 1000
```

```
S1(config-router)#neighbor 10.10.2.2 remote-as 2000
S1(config-router)#neighbor 10.10.3.2 remote-as 222
S1(config-router)#network 10.10.1.0/24
S1(config-router)#network 10.10.2.0/24
S1(config-router)#network 10.10.3.0/24
```

- Device S2 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/1
S2(config-if)#no switchport
S2(config-if)#ip address 10.10.1.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/2
S2(config-if)#no switchport
S2(config-if)#ip address 192.168.2.1/24
```

Create BGP process

```
S2#configure terminal
S2(config)#router bgp 1000
S2(config-router)#bgp confederation identifier 111
S2(config-router)#neighbor 10.10.1.1 remote-as 1000
S2(config-router)#network 192.168.2.0/24
```

- Device S3 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/1
S3(config-if)#no switchport
S3(config-if)#ip address 10.10.2.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/2
S3(config-if)#no switchport
S3(config-if)#ip address 192.168.3.1/24
```

Create BGP Process

The AS number is 2000, the confederation number is 111, and the EBGP AS number in the confederation is 1000. It is necessary to establish a fully connected neighbor relationship with all devices in the confederation.

```
S3#configure terminal
S3(config)#router bgp 2000
```

```
S3(config-router)#bgp confederation identifier 111
S3(config-router)#neighbor 10.10.1.2 remote-as 1000
S3(config-router)#neighbor 10.10.2.1 remote-as 1000
S3(config-router)#network 192.168.3.0/24
```

- Device S4 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/1
S4(config-if)#no switchport
S4(config-if)#ip address 10.10.3.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/2
S4(config-if)#no switchport
S4(config-if)#ip address 192.168.4.1/24
```

Create BGP Process

The AS number is 222, and a neighbor relationship needs to be established with the device 10.10.3.1 whose AS number is 111 (actually the AS number of the confederation).

```
S4#configure terminal
S4(config)#router bgp 222
S4(config-router)#neighbor 10.10.3.1 remote-as 111
S4(config-router)#network 192.168.4.0/24
```

- Results display

Device S1：

Display bgp neighbor information and routing table on device S1

```
S1#show ip bgp neighbors
BGP neighbor is 10.10.1.2, remote AS 1000, local AS 1000, internal link
  BGP version 4, remote router ID 10.10.1.2
  BGP state = Established, up for 02:43:59
  Last read 02:43:58, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 1316 messages, 0 notifications, 0 in queue
  Sent 1326 messages, 1 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
```

```
  BGP table version 16, neighbor version 16
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  5 announced prefixes

 Connections established 2; dropped 1
Local host: 10.10.1.1, Local port: 46323
Foreign host: 10.10.1.2, Foreign port: 179
Nexthop: 10.10.1.1
Last Reset: 02:44:35, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 10.10.2.2, remote AS 2000, local AS 1000, external link
  BGP version 4, remote router ID 192.168.3.1
  Neighbor under common administration
  BGP state = Established, up for 02:39:32
  Last read 02:39:31, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 1308 messages, 1 notifications, 0 in queue
  Sent 1312 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 16, neighbor version 16
  Index 2, Offset 0, Mask 0x4
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  5 announced prefixes

 Connections established 2; dropped 1
Local host: 10.10.2.1, Local port: 59371
Foreign host: 10.10.2.2, Foreign port: 179
Nexthop: 10.10.2.1
Last Reset: 02:40:09, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

BGP neighbor is 10.10.3.2, remote AS 222, local AS 111, external link
```

```
  BGP version 4, remote router ID 192.168.4.1
  BGP state = Established, up for 02:33:58
  Last read 02:33:57, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 184 messages, 0 notifications, 0 in queue
  Sent 187 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 16, neighbor version 16
  Index 3, Offset 0, Mask 0x8
  Community attribute sent to this neighbor (both)
  1 accepted prefixes
  5 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.3.1, Local port: 49367
Foreign host: 10.10.3.2, Foreign port: 179
Nexthop: 10.10.3.1

S1#
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
C          10.10.2.0/24 is directly connected, gigabitEthernet0/2
C          10.10.3.0/24 is directly connected, gigabitEthernet0/4
C          192.168.1.0/24 is directly connected, gigabitEthernet0/3
B          192.168.2.0/24 [200/0] via 10.10.1.2, gigabitEthernet0/1, 02:44:03
B          192.168.3.0/24 [200/0] via 10.10.2.2, gigabitEthernet0/2, 02:39:36
B          192.168.4.0/24 [20/0] via 10.10.3.2, gigabitEthernet0/4, 02:34:02
```

```
Gateway of last resort is not set
S1#
S1#show ip bgp
BGP table version is 16, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric       LocPrf       Weight
Path
*> 10.10.1.0/24     0.0.0.0                           100          32768
i
*> 10.10.2.0/24     0.0.0.0                           100          32768
i
*> 10.10.3.0/24     0.0.0.0                           100          32768
i
*>i192.168.2.0      10.10.1.2                0        100             0
i
*> 192.168.3.0      10.10.2.2                0        100             0
(2000) i
*> 192.168.4.0      10.10.3.2                0                        0
222 i

Total number of prefixes 6
S1#
```

Device S2:

Display bgp neighbor information and routing table on device S2

```
S2#show ip bgp neighbors
BGP neighbor is 10.10.1.1, remote AS 1000, local AS 1000, internal link
  BGP version 4, remote router ID 192.168.1.1
  BGP state = Established, up for 02:43:06
  Last read 00:11:33, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 1341 messages, 1 notifications, 0 in queue
  Sent 1313 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
```

```
  For address family: IPv4 Unicast
    BGP table version 3, neighbor version 2
    Index 1, Offset 0, Mask 0x2
    Community attribute sent to this neighbor (both)
    4 accepted prefixes
    1 announced prefixes

  Connections established 2; dropped 1
Local host: 10.10.1.2, Local port: 179
Foreign host: 10.10.1.1, Foreign port: 46323
Nexthop: 10.10.1.2
Last Reset: 02:43:42, due to BGP Notification received
Notification Error Message: (Cease/Other Configuration Change.)

S2#
S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
           O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
           * - candidate default

IP Route Table for VRF "default"
C           10.10.1.0/24 is directly connected, gigabitEthernet0/1
B           10.10.2.0/24 [200/0] via 10.10.1.1, gigabitEthernet0/1, 00:11:38
B           10.10.3.0/24 [200/0] via 10.10.1.1, gigabitEthernet0/1, 00:11:35
C           192.168.2.0/24 is directly connected, gigabitEthernet0/2
B           192.168.4.0/24 [200/0] via 10.10.3.2 (recursive via 10.10.1.1 ),
00:16:53

Gateway of last resort is not set
S2#
S2#show ip bgp
BGP table version is 3, local router ID is 10.10.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network             Next Hop                Metric        LocPrf        Weight
Path
```

```
*>i10.10.1.0/24      10.10.1.1                0          100          0
i
*>i10.10.2.0/24      10.10.1.1                0          100          0
i
*>i10.10.3.0/24      10.10.1.1                0          100          0
i
*> 192.168.2.0       0.0.0.0                             100        32768
i
*>i192.168.4.0       10.10.3.2                0          100          0
222 i

Total number of prefixes 5
S2#
```

Device S3:

Display bgp neighbor information and routing table on device S3

```
S3#show ip bgp neighbors
BGP neighbor is 10.10.1.2, remote AS 1000, local AS 2000, external link
  BGP version 4, remote router ID 0.0.0.0
  Neighbor under common administration
  BGP state = Connect
  Last read          , hold time is 180, keepalive interval is 60 seconds
  Received 0 messages, 0 notifications, 0 in queue
  Sent 0 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 0
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  0 accepted prefixes
  0 announced prefixes

 Connections established 0; dropped 0
Next connect timer due in 1 seconds

BGP neighbor is 10.10.2.1, remote AS 1000, local AS 2000, external link
  BGP version 4, remote router ID 192.168.1.1
  Neighbor under common administration
  BGP state = Established, up for 02:36:36
  Last read 00:09:10, hold time is 180, keepalive interval is 60 seconds
```

```
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 203 messages, 0 notifications, 0 in queue
  Sent 185 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 1
  Index 3, Offset 0, Mask 0x8
  Community attribute sent to this neighbor (both)
  5 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.2.2, Local port: 179
Foreign host: 10.10.2.1, Foreign port: 59371
Nexthop: 10.10.2.2

S3#
S3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
B       10.10.1.0/24 [200/0] via 10.10.2.1, gigabitEthernet0/1, 00:09:41
C       10.10.2.0/24 is directly connected, gigabitEthernet0/1
B       10.10.3.0/24 [200/0] via 10.10.2.1, gigabitEthernet0/1, 00:09:13
B       192.168.2.0/24 [200/0] via 10.10.1.2 (recursive via 10.10.2.1 ),
00:14:44
C       192.168.3.0/24 is directly connected, vlan200
B       192.168.4.0/24 [200/0] via 10.10.3.2 (recursive via 10.10.2.1 ),
00:14:44

Gateway of last resort is not set
S3#
```

```
S3#show ip bgp
BGP table version is 2, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf     Weight
Path
*> 10.10.1.0/24     10.10.2.1                0        100          0
(1000) i
*> 10.10.2.0/24     10.10.2.1                0        100          0
(1000) i
*> 10.10.3.0/24     10.10.2.1                0        100          0
(1000) i
*> 192.168.2.0      10.10.1.2                0        100          0
(1000) i
*> 192.168.3.0      0.0.0.0                           100      32768
i
*> 192.168.4.0      10.10.3.2                0        100          0
(1000) 222 i

Total number of prefixes 6
S3#
```

Device S4：

Display bgp neighbor information and routing table on device S4

```
S4#show ip bgp neighbors
BGP neighbor is 10.10.3.1, remote AS 111, local AS 222, external link
  BGP version 4, remote router ID 192.168.1.1
  BGP state = Established, up for 02:30:24
  Last read 00:08:38, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    Four-octets ASN Capability: advertised and received
    Address family IPv4 Unicast: advertised and received
  Received 192 messages, 1 notifications, 0 in queue
  Sent 181 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds

 For address family: IPv4 Unicast
  BGP table version 2, neighbor version 1
```

```
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (both)
  5 accepted prefixes
  1 announced prefixes

 Connections established 1; dropped 0
Local host: 10.10.3.2, Local port: 179
Foreign host: 10.10.3.1, Foreign port: 49367
Nexthop: 10.10.3.2
Last Reset: 02:31:15, due to BGP Notification received
Notification Error Message: (OPEN Message Error/Bad Peer AS.)

S4#
S4#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
B          10.10.1.0/24 [20/0] via 10.10.3.1, gigabitEthernet0/1, 00:09:03
B          10.10.2.0/24 [20/0] via 10.10.3.1, gigabitEthernet0/1, 00:08:40
C          10.10.3.0/24 is directly connected, gigabitEthernet0/1
B          192.168.2.0/24 [20/0] via 10.10.3.1, gigabitEthernet0/1, 02:30:25
B          192.168.3.0/24 [20/0] via 10.10.3.1, gigabitEthernet0/1, 02:30:25
C          192.168.4.0/24 is directly connected, gigabitEthernet0/2

Gateway of last resort is not set
S4#
S4#show ip bgp
BGP table version is 2, local router ID is 192.168.4.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
                    S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop                Metric       LocPrf       Weight
Path
*> 10.10.1.0/24       10.10.3.1                  0                         0
111 i
```

```
*> 10.10.2.0/24        10.10.3.1                0                      0
111 i
*> 10.10.3.0/24        10.10.3.1                0                      0
111 i
*> 192.168.2.0         10.10.3.1                0                      0
111 i
*> 192.168.3.0         10.10.3.1                0                      0
111 i
*> 192.168.4.0         0.0.0.0                            100         32768
i

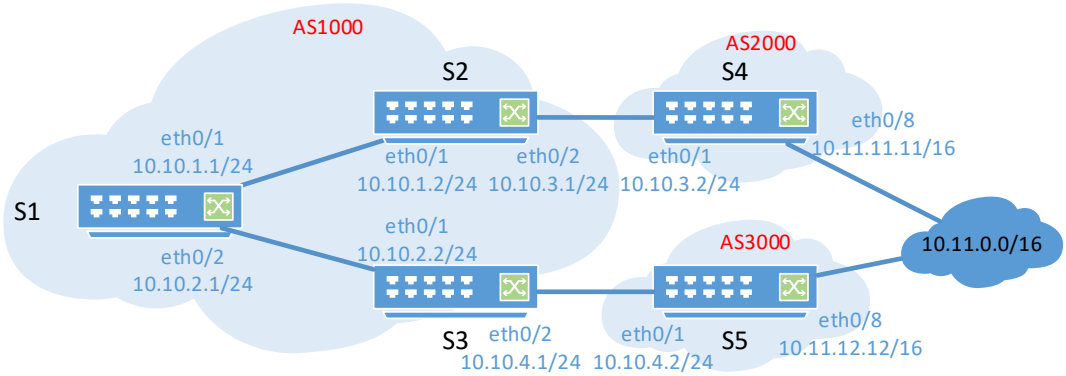
Total number of prefixes 6
S4#
```

16.3.2. Multipath load balancing configuration

Requirements

- 5 devices exchange routes using BGP protocol;
- Construct 2 multi-path load balancing scenarios;

Networking



CONFIG.Eg.

- Device S1 configuration steps

  Configure the ip address of port gigabitEthernet0/1

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/1
```

```
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.1.1/24
```

Configure the ip address of port gigabitEthernet0/2

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/2
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.2.1/24
```

Create BGP process and multi-path load configuration and AS-PATH loose comparison mode

```
S1#configure terminal
S1(config)#router bgp 1000
S1(config-router)#neighbor 10.10.1.2 remote-as 1000
S1(config-router)#neighbor 10.10.2.2 remote-as 1000
S1(config-router)#bgp bestpath as-path multipath-relax
S1(config-router)#maximum-paths ibgp 2
```

- Device S2 configuration steps

Create BGP process

```
S2#configure terminal
S2(config)#router bgp 1000
S2(config-router)#neighbor 10.10.1.1 remote-as 1000
S2(config-router)#network 10.10.3.0/24
```

Configure the ip address of port gigabitEthernet0/1

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/1
S2(config-if)#no switchport
S2(config-if)#ip address 10.10.1.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/2
S2(config-if)#no switchport
S2(config-if)#ip address 10.10.3.1/24
```

- Device S3 configuration steps

Create BGP Process

```
S3#configure terminal
S3(config)#router bgp 1000
S3(config-router)#neighbor 10.10.2.1 remote-as 1000
S3(config-router)#network 10.10.4.0/24
```

Configure the ip address of port gigabitEthernet0/1

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/1
S3(config-if)#no switchport
```

```
S3(config-if)#ip address 10.10.2.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/2
S3(config-if)#no switchport
S3(config-if)#ip address 10.10.4.1/24
```

- Device S4 configuration steps

Create BGP process

```
S4#configure terminal
S4(config)#router bgp 2000
S4(config-router)#neighbor 10.10.3.1 remote-as 1000
S4(config-router)#network 10.11.0.0/16
```

Configure the ip address of port gigabitEthernet0/1

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/1
S4(config-if)#no switchport
S4(config-if)#ip address 10.10.3.2/24
```

Configure the ip address of port gigabitEthernet0/8

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/8
S4(config-if)#no switchport
S4(config-if)#ip address 10.11.11.11/16
```

- Device S5 configuration steps

Create BGP process

```
S5#configure terminal
S5(config)#router bgp 3000
S5(config-router)#neighbor 10.10.4.1 remote-as 1000
S5(config-router)#network 10.11.0.0/16
```

Configure the ip address of port gigabitEthernet0/1

```
S5#configure terminal
S5(config)#interface gigabitEthernet0/1
S5(config-if)#no switchport
S5(config-if)#ip address 10.10.4.2/24
```

Configure the ip address of port gigabitEthernet0/8

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/8
S4(config-if)#no switchport
S4(config-if)#ip address 10.11.12.12/16
```

- Results display

Device S1：

Display bgp neighbor information and routing table on device S1. There are two routes to 10.11.0.0/16 on S1.

```
S1#show ip bgp summary
BGP router identifier 192.168.1.1, local AS number 1000
BGP table version is 23
3 BGP AS-PATH entries
0 BGP Community entries

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ
Up/Down  State/PfxRcd
10.10.1.2       4         1000    1673    1678       22    0    0
07:44:28
 2
10.10.2.2       4         1000      78      79       22    0    0
01:01:15
 2

Total number of neighbors 2
S1#
S1#
S1#show ip bgp
BGP table version is 23, local router ID is 192.168.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric     LocPrf     Weight
Path
*> 10.10.1.0/24     0.0.0.0                        100        32768
i
*> 10.10.2.0/24     0.0.0.0                        100        32768
i
*>i10.10.3.0/24     10.10.1.2                0     100             0
i
*>i10.10.4.0/24     10.10.2.2                0     100             0
i
*>i10.11.0.0/16     10.10.3.2                0     100             0
2000 i
* i                  10.10.4.2                0     100             0
3000 i
```

```
Total number of prefixes 5
S1#
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
C          10.10.2.0/24 is directly connected, gigabitEthernet0/2
B          10.10.3.0/24 [200/0] via 10.10.1.2, gigabitEthernet0/1, 00:12:05
B          10.10.4.0/24 [200/0] via 10.10.2.2, gigabitEthernet0/2, 00:10:30
B          10.11.0.0/16 [200/0] via 10.10.4.2 (recursive via 10.10.2.2 ),00:10:24
                        [200/0] via 10.10.3.2 (recursive via 10.10.1.2 ),00:10:24

Gateway of last resort is not set
S1#
```

16.4. DISPLAY COMMAND

```
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
C          10.10.2.0/24 is directly connected, gigabitEthernet0/2
B          10.10.3.0/24 [200/0] via 10.10.1.2, gigabitEthernet0/1, 00:12:05
B          10.10.4.0/24 [200/0] via 10.10.2.2, gigabitEthernet0/2, 00:10:30
B          10.11.0.0/16 [200/0] via 10.10.4.2 (recursive via 10.10.2.2 ),00:10:24
                        [200/0] via 10.10.3.2 (recursive via 10.10.1.2 ),00:10:24

Gateway of last resort is not set
S1#
```

- Only display BGP routing information

```
S1#show ip route bgp
IP Route Table for VRF "default"
B          10.10.3.0/24 [200/0] via 10.10.1.2, gigabitEthernet0/1, 00:14:20
B          10.10.4.0/24 [200/0] via 10.10.2.2, gigabitEthernet0/2, 00:12:45
B          10.11.0.0/16 [200/0] via 10.10.4.2 (recursive via 10.10.2.2 ),00:12:39
                        [200/0] via 10.10.3.2 (recursive via 10.10.1.2 ),00:12:39

Gateway of last resort is not set
S1#
```

- Other BGP information

Command	Function
show ip bgp	Displays general information about BGP
show ip bgp summary	Display BGP connection summary information
show ip bgp neighbors	Display BGP neighbor details
show ip bgp paths	Display BGP path information

17. CONFIGURE IS-IS

17.1. IS-IS OVERVIEW

IS-IS (Intermediate System-to-Intermediate System, Intermediate System to Intermediate System) is a routing protocol, suitable for dual-environment networks of IP and ISO CLNS, is a scalable, robust, easy-to-use IGP protocol.

IS-IS, as a link state protocol, has the commonality of link state protocols. It discovers and maintains neighbor relationships by sending Hello packets, and advertises its own link status by sending protocol datagrams LSP (Link State PDU) to neighbors. IS-IS supports layer 2 routing (layer 1 and layer 2 routing) scheme, all devices in the same layer have the same LSDB, and the LSDB stores the LSPs generated by all devices in the same layer, so that all devices in the same layer know themselves Depending on the network topology at the level, each device uses the Dijkstra Shortest Path First (SPF) algorithm to optimize route calculation, path selection and achieve fast convergence.

17.2. CONFIG.COMMAND

17.2.1. **Create IS-IS process**

To run the IS-IS routing protocol, first create an IS-IS routing process in the global configuration mode. The router isis can carry the parameter Tag, which is a name used to represent the IS-IS routing process. Configure different IS-IS routing processes by adding different tags.

After the IS-IS process is started, a system ID needs to be set for IS-IS to uniquely identify the IS-IS instance in the entire autonomous domain.

System ID and NET in configuration commands can be divided into three parts: area address, System ID, and NSAP identification. The total length is 8-20 bytes.

- The area address identifies the length of the routing domain of the area and is fixed in the routing domain. Length is 1-13 bytes.
- The System ID is unique in the autonomous system.
- NSAP is the network selector, sometimes called SEL. In IS-IS, SEL is always set to 00 to indicate router.

In IS-IS, each area can contain one or more area addresses, usually only one area address needs to be configured. When re-dividing the area, it can be achieved by configuring multiple area addresses. When configuring multiple zone addresses in one IS, the system ID part must be the same.

Command	SWITCH(config)#**router isis** [*tag*] SWITCH(config-router)# **net** *NET*

Description	Create a process and configure a unique ID.

17.2.2. **Enable IS-IS**

Command	SWITCH(config-if)#**iprouter isis** [*tag*]
Description	Enable the isis function on the interface. tag represents the process name of isis.

17.2.3. Protocol packet parameter configuration

- Configure the hello packet interval

Command	SWITCH(config-if)#**isis hello-interval** {*seconds* | minimal} {level-1 | level-2}
Description	hello-interval is used to set the interval for sending hello packets on the interface. The value of the two ends of the neighbor must be the same. seconds is the interval value, the unit is seconds, the range is 1-65535, and the default value is 10. The function of the minimal parameter is to set the holdtime to 1, and the value of the hello interval will be calculated by the hello-multiplier. For example, if hello-multiplier is set to 3, and isis hello-interval minimal is set, the value of hello-interval should be 1/3 of a second (333 milliseconds). After the minimal parameter is configured, the number of hello packets exchanged between devices will greatly increase, and the processing burden of the device will also increase greatly. If the device performance is low or the load is already heavy, neighbors may flap. The level-1/level-2 parameters indicate different levels. If not selected, the same configuration is applied to different levels.

- Configure the multiple of hello packet holdtime

Command	SWITCH(config-if)#**isis hello-multiplier** *value* [level-1 | level-2]
Description	value is used to set the holdtime multiple of the hello packet on the interface, thereby modifying the holdtime value in the hello packet. The holdtime value in the packet is equal to the product of hello-interval and hello-multiplier. The default value is 3.

- Configuring the interval for sending LSP packets

Command	SWITCH(config-if)#**isis lsp-interval** *interval*
Description	interval is the shortest interval for transmitting LSP packets on the interface, in milliseconds, and the range is 1 - 4294967295.

- Configuring the retransmission interval of LSP packets

Commanf	SWITCH(config-if)#**isis retransmit-interval** *interval*
Description	interval is the interval for retransmission of LSP packets transmitted on the interface. The unit is seconds, and the range is 1 - 65535.

- Configuring the LSP refresh interval

Command	SWITCH(config-router)#**lsp-refresh-interval** *seconds*
Description	second is used to set the refresh interval of LSP, the unit is second, the range is 1 - 65535. The set value of lsp-refresh-interval must be less than the set value of max-lsp-lifetime.

- Configure the valid time of LSP packets

Command	SWITCH(config-router)#**max-lsp-lifetime** *seconds*
Description	second is used to set the valid time of LSP, the unit is second, the range is 1 - 65535. The setting value of max-lsp-lifetime must be greater than the setting value of lsp-refresh-interval.

- Ignore LSP packet verification

Command	SWITCH(config-router)#**ignore-lsp-errors**
Description	Used to set checksum errors to ignore LSPs.

- Configuring the broadcast interval of CSNP packets

Command	SWITCH(config-if)#**isis csnp-interval** *seconds* [level-1 | level-2]
Description	Used to set the interval for sending CSNP packets on the interface, in seconds, ranging from 1 to 65535. The default value is 10. If set to 0, it means that CSNP packets are not sent.

17.2.3.IS-IS Hierarchical Configuration

Command	SWITCH(config-router)#**is-type** {level-1 | level-1-2 | level-2-only}
Description	Used to set the hierarchy type of the IS-IS system. level-1 is used to represent routers within an area, level-2 is used to represent routers between areas, and level-1-2 is used to represent border routers that are both intra-area routers and inter-area routers.

It is also possible to configure the hierarchy of is-is based on the interface.

Command	SWITCH(config-if)#**isis circuit-type** {level-1 | level-1-2 | level-2-only}
Description	An interface configured with the isis level can only send protocol packets of the corresponding level.

17.2.3.IS-IS Authentication Configuration

Unsupported so far .

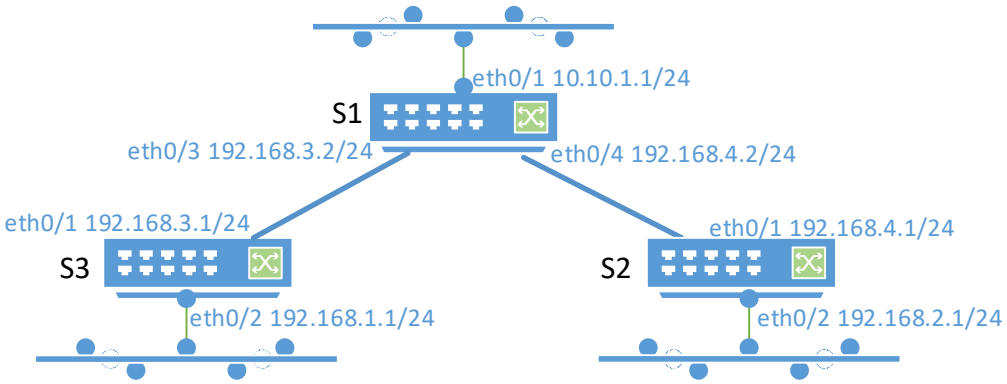
17.3. CONFIGURE CASE

17.3.1. IS-IS Basic configuration

Requirements

- 3 devices exchange routes using ISIS protocol;
- S1 does not advertise the routes of the 10.10.1.1/24 network segment; S2, S3 advertise all routes of the local machine
- Each device can learn all advertised routes in the autonomous domain

Networking



1) Config.Eg.

- Device S1 configuration steps

Create IS-IS process

```
S1#configure terminal
S1(config)#router isis 1
S1(config-router)#net 66.0001.0000.0000.0001.00
```

Configure the ip address of port gigabitEthernet0/1. Because isis is not enabled, this network segment will not be published by the isis protocol.

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/1
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.1.1/24
```

Configure the ip address of port gigabitEthernet0/3 and enable is-is

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/3
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.3.2/24
S1(config-if)#ip router isis 1
```

Configure the ip address of port gigabitEthernet0/4 and enable is-is

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/4
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.4.2/24
S1(config-if)#ip router isis 1
```

- Device S2 configuration steps

Create ISIS process

```
S2#configure terminal
S2(config)#router isis 1
S2(config-if)#net 66.0001.0000.0000.0002.00
```

Configure the ip address of port gigabitEthernet0/3 and enable isis

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/1
S2(config-if)#no switchport
S2(config-if)#ip address 192.168.4.1/24
S2(config-if)#ip router isis 1
```

Configure the ip address of port gigabitEthernet0/4 and enable isis

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/2
S2(config-if)#no switchport
S2(config-if)#ip address 192.168.2.1/24
S2(config-if)#ip router isis 1
```

- Device S3 configuration steps

Create ISIS process

```
S3#configure terminal
S3(config)#router isis 1
S3(config-if)#net 66.0001.0000.0000.0002.00
```

Configure the ip address of port gigabitEthernet0/1 and enable isis

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/1
S3(config-if)#no switchport
S3(config-if)#ip address 192.168.3.1/24
S3(config-if)#ip router isis 1
```

Configure the ip address of port gigabitEthernet0/2 and enable isis

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/2
S3(config-if)#no switchport
S3(config-if)#ip address 192.168.1.1/24
```

```
S3(config-if)#ip router isis 1
```

- Results display

Device S1:

Display routing table on device S1

```
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
i L1    192.168.1.0/24 [115/20] via 192.168.3.1, gigabitEthernet0/3, 00:01:02
i L1    192.168.2.0/24 [115/20] via 192.168.4.1, gigabitEthernet0/4, 00:00:12
C          192.168.3.0/24 is directly connected, gigabitEthernet0/3
C          192.168.4.0/24 is directly connected, gigabitEthernet0/4

Gateway of last resort is not set
S1#
```

Device S2:

Display routing table on device S

```
S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
i L1    192.168.1.0/24 [115/30] via 192.168.4.2, gigabitEthernet0/1, 00:00:55
C          192.168.2.0/24 is directly connected, gigabitEthernet0/2
i L1    192.168.3.0/24 [115/20] via 192.168.4.2, gigabitEthernet0/1, 00:08:48
C          192.168.4.0/24 is directly connected, gigabitEthernet0/1

Gateway of last resort is not set
S2#
```

Device S3:

Display routing table on device S3

```
S3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          192.168.1.0/24 is directly connected, gigabitEthernet0/2
i L1    192.168.2.0/24 [115/30] via 192.168.3.2, gigabitEthernet0/1, 00:01:45
C          192.168.3.0/24 is directly connected, gigabitEthernet0/1
i L1    192.168.4.0/24 [115/20] via 192.168.3.2, gigabitEthernet0/1, 00:10:25

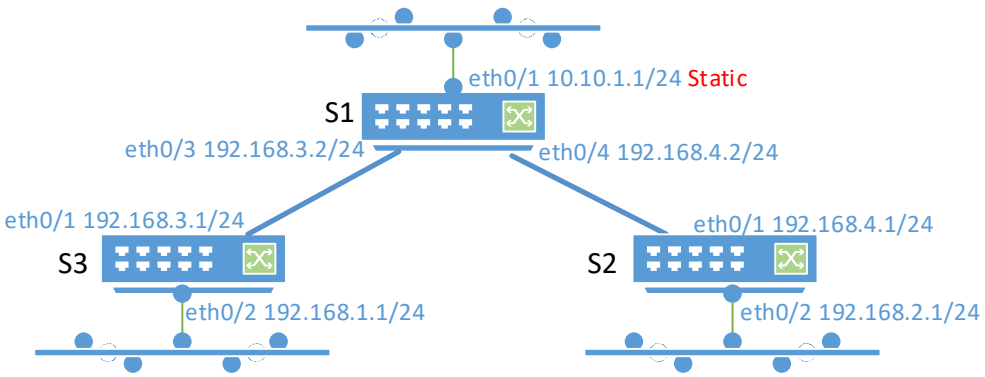
Gateway of last resort is not set
S3#
```

17.3.2.IS-IS route redistribution configuration

Requirements

- 3 devices exchange routes using ISIS protocol;
- □S1 does not advertise the route of the 10.10.1.1/24 network segment, configure a static route to the 112.0.0./6 network segment, the next hop is 10.10.1.2, and re-advertise this route through the ISIS protocol;
- □S2, S3 publish all routes of the machine
- □Each device can learn all the advertised routes in the autonomous domain, including the static routes of S1

Networking



Config.Eg.

Interface IP, ISIS basic configuration see the configuration example in chapter 21.3.1 ISIS basic configuration. For increasing the static route of S1 and the static route redistribution configuration in the ISIS process.

Configure static routes

```
S1#configure terminal
S1(config)#ip route 112.0.0.0/6 10.10.1.2
```

Configure the ip address of port gigabitEthernet0/4 and enable isis

```
S1#configure terminal
S1(config)#router isis 1
S1(config-router)#redistribute static
```

- Results display

Device S1:

Display routing table on device S1

```
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
S          112.0.0.0/6 [1/0] via 10.10.1.2, gigabitEthernet0/1
i L1     192.168.1.0/24 [115/20] via 192.168.3.1, gigabitEthernet0/3, 00:01:02
i L1     192.168.2.0/24 [115/20] via 192.168.4.1, gigabitEthernet0/4, 00:00:12
C          192.168.3.0/24 is directly connected, gigabitEthernet0/3
C          192.168.4.0/24 is directly connected, gigabitEthernet0/4

Gateway of last resort is not set
S1#
```

Device S2:

Display routing table on device S2

```
S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
```

```
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default

IP Route Table for VRF "default"
i L2      112.0.0.0/6 [115/10] via 192.168.4.2, gigabitEthernet0/1, 00:01:58
i L1      192.168.1.0/24 [115/30] via 192.168.4.2, gigabitEthernet0/1, 00:07:41
C           192.168.2.0/24 is directly connected, gigabitEthernet0/2
i L1      192.168.3.0/24 [115/20] via 192.168.4.2, gigabitEthernet0/1, 00:08:01
C           192.168.4.0/24 is directly connected, gigabitEthernet0/1

Gateway of last resort is not set
S2#
```

Device S3：

Display routing table on device S3

```
S3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
          O - OSPF, IA - OSPF inter area
          N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
          E1 - OSPF external type 1, E2 - OSPF external type 2
          i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
          * - candidate default

IP Route Table for VRF "default"
i L2      112.0.0.0/6 [115/10] via 192.168.3.2, gigabitEthernet0/1, 00:01:37
C           192.168.1.0/24 is directly connected, gigabitEthernet0/2
i L1      192.168.2.0/24 [115/30] via 192.168.3.2, gigabitEthernet0/1, 00:07:43
C           192.168.3.0/24 is directly connected, gigabitEthernet0/1
i L1      192.168.4.0/24 [115/20] via 192.168.3.2, gigabitEthernet0/1, 00:07:43

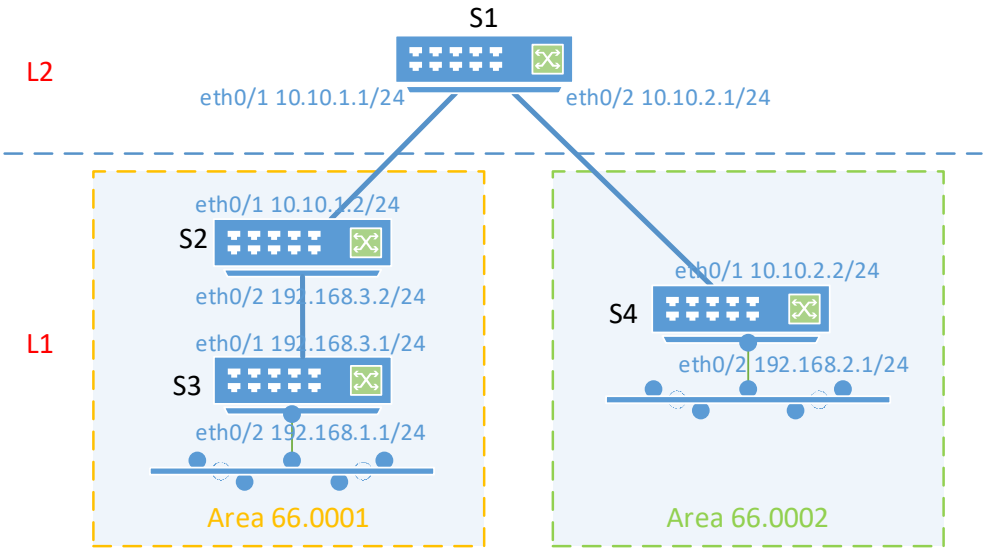
Gateway of last resort is not set
S3#
```

17.3.2. IS-IS Hierarchical Configuration

Requirements

- 4 devices exchange routes using ISIS protocol;
- S2 and S3 are in the same autonomous domain; S4 is in the same autonomous domain; S1 does the IS-IS area route summary;

Networking



Config.Eg.

- Device S1 configuration steps

Create an ISIS process and configure S1 to run only at level 2, so that S1 only cares about changes in the topology of IS-IS at level 2, that is, routing changes.

```
S1#configure terminal
S1(config)#router isis 1
S1(config-router)#net 88.0001.0000.0000.0001.00
S1(config-router)#is-type level-2-only
```

Configure the ip address of port gigabitEthernet0/1 and enable isis

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/1
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.1.1/24
S1(config-if)#ip router isis 1
```

Configure the ip address of port gigabitEthernet0/2 and enable isis

```
S1#configure terminal
S1(config)#interface gigabitEthernet0/2
S1(config-if)#no switchport
S1(config-if)#ip address 10.10.2.1/24
S1(config-if)#ip router isis 1
```

- Device S2 configuration steps

Create an ISIS process. Since S1 only runs on level 2 and S3 only runs on level 1, S2 needs to support both level 1 and level 2. The default configuration is to support both level 1 and level 2, so no special configuration is required.

```
S2#configure terminal
```

```
S2(config)#router isis 1
S2(config-router)#net 66.0001.0000.0000.0002.00
```

Configure the ip address of port gigabitEthernet0/1 and enable isis

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/1
S2(config-if)#no switchport
S2(config-if)#ip address 10.10.1.2/24
S2(config-if)#ip router isis 1
```

Configure the ip address of port gigabitEthernet0/2 and enable isis

```
S2#configure terminal
S2(config)#interface gigabitEthernet0/2
S2(config-if)#no switchport
S2(config-if)#ip address 192.168.3.2/24
S2(config-if)#ip router isis 1
```

- Device S3 configuration steps

To create an ISIS process, you need to configure S3 to run only at level 1.

```
S3#configure terminal
S3(config)#router isis 1
S3(config-router)#net 66.0001.0000.0000.0003.00
S3(config-router)# is-type level-1
```

Configure the ip address of port gigabitEthernet0/1 and enable isis

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/1
S3(config-if)#no switchport
S3(config-if)#ip address 192.168.3.1/24
S3(config-if)#ip router isis 1
```

Configure the ip address of port gigabitEthernet0/2 and enable isis

```
S3#configure terminal
S3(config)#interface gigabitEthernet0/2
S3(config-if)#no switchport
S3(config-if)#ip address 192.168.1.1/24
S3(config-if)#ip router isis 1
```

- Device S4 configuration steps

To create an ISIS process, S4 needs to support both level1 and level2. The default configuration is to support both level1 and level2, so no special configuration is required.

```
S4#configure terminal
S4(config)#router isis 1
S4(config-router)#net 66.0001.0000.0000.0004.00
```

Configure the ip address of port gigabitEthernet0/1 and enable isis

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/1
S4(config-if)#no switchport
S4(config-if)#ip address 10.10.2.1/24
S4(config-if)#ip router isis 1
```

Configure the ip address of port gigabitEthernet0/2 and enable isis

```
S4#configure terminal
S4(config)#interface gigabitEthernet0/2
S4(config-if)#no switchport
S4(config-if)#ip address 192.168.2.1/24
S4(config-if)#ip router isis 1
```

- Results display .

Device S1：

Display routing table on device S1

```
S1#show isis peer

Area 1:
System Id           Type   Interface          IP Address          State   Holdtime
Circuit
0000.0000.0002   L2     GiE0/1               10.10.1.2           Up      8
0000.0000.0002.01
0000.0000.0004   L2     GiE0/2               10.10.2.2           Up      28
0000.0000.0001.03
S1#
S1#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
C          10.10.2.0/24 is directly connected, gigabitEthernet0/2
i L2    192.168.2.0/24 [115/20] via 10.10.2.2, gigabitEthernet0/2, 00:13:10
i L2    192.168.3.0/24 [115/20] via 10.10.1.2, gigabitEthernet0/1, 00:13:35

Gateway of last resort is not set
```

```
S1#
```

Device S2:

Display routing table on device S2

```
S2#show isis peer

Area 1:
System Id           Type   Interface          IP Address          State   Holdtime
Circuit
0000.0000.0001      L2     GiE0/1               10.10.1.1           Up      27
0000.0000.0002.01
0000.0000.0003      L1     GiE0/2               192.168.3.1         Up      8
0000.0000.0003.01
S2#
S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
i L2       10.10.2.0/24 [115/20] via 10.10.1.1, gigabitEthernet0/1, 00:14:37
i L1       192.168.1.0/24 [115/20] via 192.168.3.1, gigabitEthernet0/2, 00:14:04
i L2       192.168.2.0/24 [115/30] via 10.10.1.1, gigabitEthernet0/1, 00:13:49
C          192.168.3.0/24 is directly connected, gigabitEthernet0/2

Gateway of last resort is not set
S2#
```

Device S3:

Display routing table on device S3

```
S3#show isis peer

Area 1:
System Id           Type   Interface          IP Address          State   Holdtime
Circuit
0000.0000.0002      L1     GiE0/1               192.168.3.2         Up      28
0000.00
00.0003.01
S3#
```

```
S3#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 192.168.3.2 to network 0.0.0.0

i*L1    0.0.0.0/0 [115/10] via 192.168.3.2, gigabitEthernet0/1, 02:39:19
i L1    10.10.1.0/24 [115/20] via 192.168.3.2, gigabitEthernet0/1, 00:15:36
C         192.168.1.0/24 is directly connected, gigabitEthernet0/2
C         192.168.3.0/24 is directly connected, gigabitEthernet0/1
S3#
```

Device S4：

Display routing table on device S4

```
S4#show isis peer

Area 1:
System Id          Type   Interface          IP Address          State   Holdtime
Circuit
0000.0000.0001   L2     GiE0/1               10.10.2.1             Up       8
0000.0000.0001.03
S4#
S4#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
i L2    10.10.1.0/24 [115/20] via 10.10.2.1, gigabitEthernet0/1, 00:15:57
C         10.10.2.0/24 is directly connected, gigabitEthernet0/1
C         192.168.2.0/24 is directly connected, gigabitEthernet0/2
i L2    192.168.3.0/24 [115/30] via 10.10.2.1, gigabitEthernet0/1, 00:15:47

Gateway of last resort is not set
```

```
S4#
```

17.4. DISPLAY COMMAND

- Display routing information

```
S2#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
i L2       10.10.2.0/24 [115/20] via 10.10.1.1, gigabitEthernet0/1, 00:14:37
i L1       192.168.1.0/24 [115/20] via 192.168.3.1, gigabitEthernet0/2,
00:14:04
i L2       192.168.2.0/24 [115/30] via 10.10.1.1, gigabitEthernet0/1, 00:13:49
C          192.168.3.0/24 is directly connected, gigabitEthernet0/2

Gateway of last resort is not set
S2#
```

- Only display IS-IS routing information

```
S2#show ip route isis
IP Route Table for VRF "default"
i L2       10.10.2.0/24 [115/20] via 10.10.1.1, gigabitEthernet0/1, 00:20:03
i L2       112.0.0.0/6 [115/10] via 10.10.1.1, gigabitEthernet0/1, 00:20:03
i L1       192.168.1.0/24 [115/20] via 192.168.3.1, gigabitEthernet0/2, 00:19:30
i L2       192.168.2.0/24 [115/30] via 10.10.1.1, gigabitEthernet0/1, 00:19:15

Gateway of last resort is not set
S2#
```

- Other IS-IS information

Command	Function
show isis tag	Displays brief information about the processes corresponding to IS-IS
show isis topology	Display IS-IS topology information
show isis database	Display IS-IS database information
show isis interface	Display information about IS-IS interfaces
show isis peer	Display IS-IS neighbor information

18. CONFIG.RIP

18.1. RIP OVERVIEW

RIP (Routing Information Protocol) routing protocol is a routing protocol using distance vector algorithm, mainly used in small networks. There are two versions, RIPv1 and RIPv2, respectively (RIPv1 is defined in RFC 1058, and RIPv2 is defined in RFC 2453).

The RIP protocol packet is based on the UDP protocol, and the UDP port number is 520. RIPv1 packets are generally in the form of broadcast packets; RIPv2 packets are in the form of multicast packets, and the multicast address is 224.0.0.9;

The RIP protocol sends out update packets every 30 seconds. If the router does not receive a routing update packet from the peer end within 180 seconds, the machine will mark all routes from the peer device as unreachable. If the update message is not received after that, the routes advertised by the peer device may be deleted from the routing table.

RIP's routing metric refers to the number of hops used to measure the distance to a destination. The hop count of the directly connected network is marked as 0, the reachable network hop count of each device is 1; the hop count of the unreachable network is 16.

The RIP routing process will only send update packets to the network interface associated with the process.

18.2. CONFIG. COMMAND

18.2.1. **Create RIP Process**

Command	SWITCH(config)#router rip
	SWITCH(config-router)# network IP(A.B.C.D) MASK(A.B.C.D)

Description	To run the RIP routing protocol, you need to create a RIP routing process and associate the corresponding network with the RIP routing process. The router rip command creates a RIP routing process. The network command indicates the routing information of the associated network advertised by the rip command, and also indicates that the protocol advertisement and routing information update are only performed on the interface corresponding to the associated network.

	IP and MASK together form the address range.

18.2.2. RIP message update unicast announcement

Command	SWITCH(config)#router rip
	SWITCH(config-router)# neighbor IP(A.B.C.D)

Description	RIP routing protocols usually use broadcast or multicast packets for interaction, but can also support the configuration of packet update unicast advertisements to use unicast packets to update routing information. For example, this configuration is required in non-broadcast networks.

18.2.2. Configuring the RIP version

The product supports versions 1 and 2 of RIP. Version 2 supports authentication, route aggregation, and key management.

By default the product can receive version 1 and version 2 RIP packets, but will only send version 1 packets.

The product supports data packets of the RIP version that are specified to be received and sent based on the whole machine or specified based on ports.

The whole machine specifies the RIP version:

Command	SWITCH(config)#router rip SWITCH(config-router)# version {1|2}
Description	This command can be used to specify that the device only receives and sends packets of the specified version.

Specify the RIP version sent based on the port:

Command	SWITCH(config-if)# ip rip send version {1|2} {1|2}
Description	This command can be used to specify that the port only sends packets of the specified version.

Specify the received RIP version based on the port:

Command	SWITCH(config-if)# ip rip receive version {1|2} {1|2}
Description	This command can be used to specify that the port only sends packets of the specified version.

18.2.2. Route republishing configuration

Command	SWITCH(config-router)# redistribute {bgp | connected | isis [area-tag] | ospf process-id | rip | static} [metric value] [metric-type {1 | 2}] [route-map map-name] [subnets] [tag value]
Description	This command is used to configure the import of external routes (including other OSPF processes/static routes/routes of other routing protocols) to the OSPF process on the ASBR.

18.2.2. **Configuring Route Aggregation**

When a subnet route traverses the network boundary of a classful route, the subnet route can be aggregated into a classful network route, which can improve the scalability and effectiveness of the network. This can greatly reduce the size of the routing table. RIP version 2 automatically performs route aggregation by default, but version 1 does not support this function.

Command	SWITCH(config)#router rip SWITCH(config-router)#[no] auto-summary
Description	auto-summary indicates that automatic route aggregation is enabled. The no keyword indicates that automatic route aggregation is disabled.

18.2.3. Configuring Split Horizon

Due to its own mechanism, the distance vector routing protocol often causes routing loops when multiple devices are connected to an IP broadcast type network. The split horizon mechanism is used to avoid the formation of routing loops.

The split horizon mechanism optimizes the exchange of routing information between multiple devices by preventing certain routing information from being advertised from the interface that has learned the routing information. However, for non-broadcast multi-access networks (such as X.25 networks, frame relay networks, etc.), this mechanism cannot learn complete routing information because advertisements are blocked, so it is not suitable for enabling split horizon.
Poison reversal is an improved mechanism of split horizon technology. When split horizon with poison reversal is enabled, the interface that has learned routing information will still advertise the routing information, but will set the metric attribute in the routing information. In this way, after receiving this kind of routing information, the peer end will immediately discard the route without waiting for its aging time, which will speed up the convergence of the route.

Split horizon is configured in interface mode.

Command	SWITCH(config-if)#[no] ip rip split-horizon {poisoned-reverse}

Description	The split-horizon keyword indicates that the horizontal split of the rip is enabled. The poisoned-reverse keyword indicates poison reverse.

18.2.3. Configuring RIP Authentication

Unsupported so far.

18.2.3. Configuring RIP Timer

There are three timers in the RIP protocol (all in seconds):

Route update timer: This timer is used to define the interval for the device to send route update packets. The default interval is 30 seconds.

Route invalidation timer: This timer is used to define how long the route in the routing table is not updated before it becomes invalid. The default period is 180 seconds.

Route clearing timer: This timer is used to set the time after which invalid routes are cleared from the routing table. The default period is 120 seconds.

Command	SWITCH(config)#router rip SWITCH(config-router)#timer basic update-time invalid-time flush-timer
Description	The update-time keyword indicates the route update time. The invalid-time keyword indicates the invalid time of the route. The flush-time keyword indicates the route clearing time.

18.2.3. **Configuring RIP source address verification**

By default, the RIP protocol will check the source address of the received routing update packet. For the packet with an invalid source address, the protocol will discard the packet. The criterion for judging is whether the source address of the received packet matches the The IP address of the receiving interface is in the same network, and the function can be disabled through configuration.

Command	SWITCH(config)#router rip SWITCH(config-router)#[no] validate-update-source
Description	Keyword “no” indicates that source address verification is disabled.

18.2.4. **Configure Interface**

In passive interface mode, the port can be configured to only learn RIP routes without advertising RIP routes.

Command	SWITCH(config)#router rip SWITCH(config-router)#[no] passive-interface {default | interface-name}
Description	The keyword “no” means to close the passive interface. The keyword “default” indicates that it applies to all interfaces. The keyword ″ interface-name″ indicates that it applies to the specified interface.

In interface mode, the interface can be specified to allow/disable the receiving/sending of rip packets.

Command	SWITCH(config-if)#[no] ip rip {send | receive} enable
Description	The keyword “send” indicates the sending of rip packets. The keyword “receive” indicates the reception of rip packets.

18.2.5. Configuring Supernet Routing

A supernet route is a route whose mask length is less than the natural mask length. Since RIP version 1 does not support receiving supernet routes, if the interface of the RIP version 1 routing device is interconnected with the RIP version 2 routing device, when the version 1 device receives the updated version with the supernet route, it will send the information in the routing information. The subnet mask is ignored, which will cause route learning errors. In order to be compatible with such situations, the device supports configuring the interface to prohibit sending supernet route advertisements.

Command	SWITCH(config-if)#[no] ip rip send supernet-routes
Description	no means that the sending of supernet routes is prohibited.

Note: Ports that only receive version 1 packets do not support receiving supernet routes, and ports that only send version 1 packets will not send supernet routes. Interfaces that support version 2 support both sending and interface supernet routes; Routes are not automatically aggregated.

18.2.5. **Configuring Default Route Advertisement**

A default route can be generated based on the interface-specified route update message. You can also specify that only the default route is passed without advertising other routes.

Command	SWITCH(config-if)#ip rip default-information {originate | only} [metric metric-value] SWITCH(config-if)#no ip rip default-information

Description	The originate keyword indicates that in addition to advertising the default route, other routes are also advertised. The only keyword indicates that only the default route of the interface is advertised, and no other routes are advertised.

Note: Between the default-information configured in the RIP process and the ip rip default-information configured under the interface, the interface configuration has a higher priority than the RIP process configuration, that is, if both exist, the default route configured under the interface is advertised.

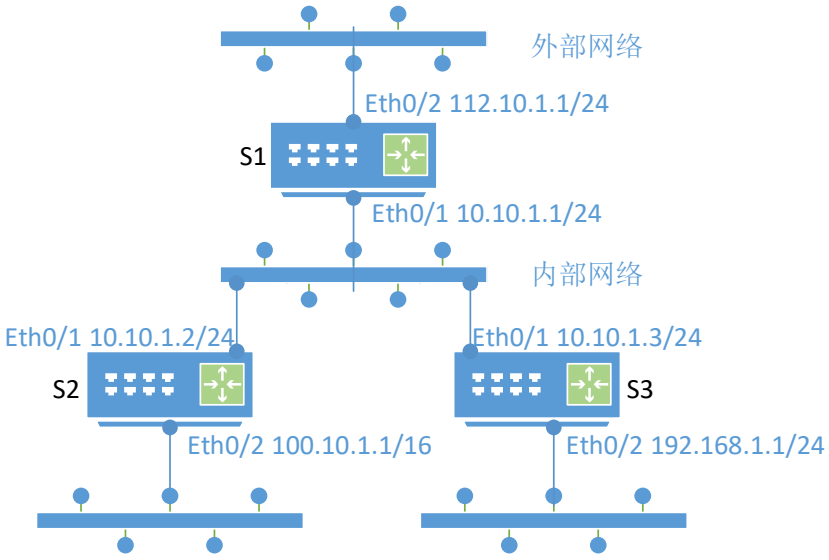
18.3. CONFIG.CASE

18.3.1. RIP routing configuration

Requirements

- Routes between all devices automatically adapt to network changes.
- □ The switch connected to the external network receives routes advertised by the external network, but does not advertise routes to the external network.
- □ Can advertise routes with subnet masks.

Networking



Configgure case

- Device S1 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.1.1/24
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 112.10.1.1/24
```

Configure the RIP process

Enable the rip process and configure the RIP version to version 2 so that routes with subnet masks can be advertised.

Since the gigabitEthernet0/2 port of S1 is connected to the external network, in order to meet the requirement of receiving external network routes but not advertising routes to the external network, you need to configure the gigabitEthernet0/2 port as a passive interface.

The internal network needs to learn specific subnet routes, so the default route aggregation needs to be turned off.

```
SWITCH(config)#router rip
SWITCH(config-router)#version 2
SWITCH(config-router)#passive-interface gigabitEthernet0/2
SWITCH(config-router)#no auto-summary
```

Associated Network

```
SWITCH(config-router)#network 10.10.1.0 255.255.255.0
SWITCH(config-router)#network 112.10.1.1 255.255.255.0
```

- Device S2 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.1.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 100.10.1.1/16
```

Configure the RIP process

Enable the rip process and configure the RIP version to version 2 so that routes with subnet masks can be advertised.

The internal network needs to learn specific subnet routes, so the default route aggregation needs to be turned off.

```
SWITCH(config)#router rip
SWITCH(config-router)#version 2
SWITCH(config-router)#no auto-summary
```

Associated Network

```
SWITCH(config-router)#network 10.10.1.0 255.255.255.0
SWITCH(config-router)#network 100.10.1.1 255.255.0.0
```

- Device S3 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.1.3/24
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 192.168.1.1/24
```

Configure the RIP process

Enable the rip process and configure the RIP version to version 2 so that routes with subnet masks can be advertised.

The internal network needs to learn specific subnet routes, so the default route aggregation needs to be turned off.

```
SWITCH(config)#router rip
SWITCH(config-router)#version 2
SWITCH(config-router)#no auto-summary
```

Associated Network

```
SWITCH(config-router)#network 10.10.1.0 255.255.255.0
SWITCH(config-router)#network 192.168.1.0 255.255.255.0
```

- Results display

Device S1：

Display routing table on device S1

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
R          100.10.0.0/16 [120/1] via 10.10.1.2, gigabitEthernet0/1, 00:17:08
C          112.10.1.0/24 is directly connected, gigabitEthernet0/2
R          192.168.1.0/24 [120/1] via 10.10.1.3, gigabitEthernet0/1, 00:18:07

Gateway of last resort is not set
```

Device S2：

Display routing table on device S2

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
C          100.10.0.0/16 is directly connected, gigabitEthernet0/2
R          112.10.1.0/24 [120/1] via 10.10.1.1, gigabitEthernet0/1, 00:18:57
R          192.168.1.0/24 [120/1] via 10.10.1.3, gigabitEthernet0/1, 00:19:59
Gateway of last resort is not set
```

Device S3：

Display routing table on device S3

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default
IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
```

```
R        100.10.0.0/16 [120/1] via 10.10.1.2, gigabitEthernet0/1, 00:19:26
R        112.10.1.0/24 [120/1] via 10.10.1.1, gigabitEthernet0/1, 00:19:23
C        192.168.1.0/24 is directly connected, gigabitEthernet0/2
Gateway of last resort is not set
SWITCH#
```

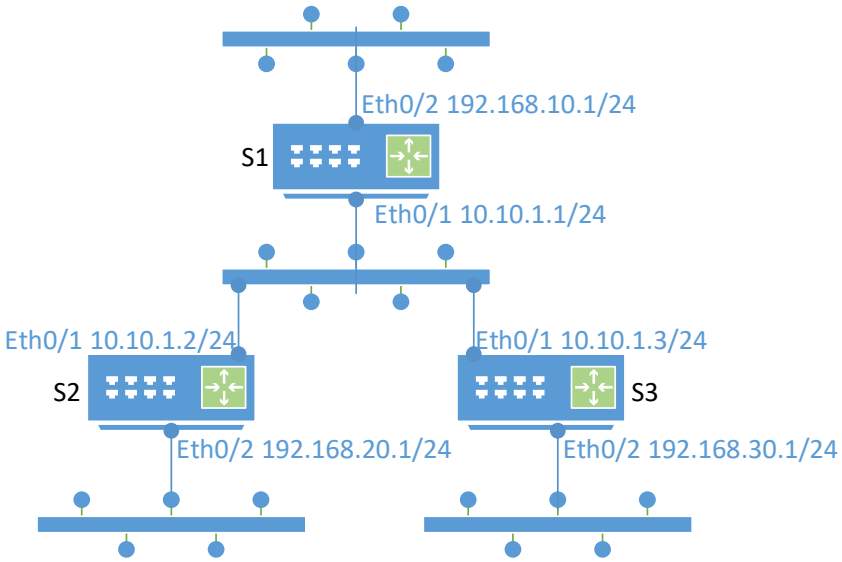
18.3.2. RIP Unicast Advertisement Configuration

Requirements

Three LAN switches S1, S2, S3:

- S1 can learn the routes of S2 and S3
- S3 can learn the routes of S1 and S3
- S2 cannot learn the routes of S3

Networking



Configure Case

- Device S1 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.1.1/24
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
```

```
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 192.168.10.1/24
```

Configure the RIP process

Enable the rip process and configure the RIP version to version 2 so that routes with subnet masks can be advertised.

Since the gigabitEthernet0/2 port of S1 is connected to the external network, in order to meet the requirement of receiving external network routes but not advertising routes to the external network, you need to configure the gigabitEthernet0/2 port as a passive interface.

The internal network needs to learn specific subnet routes, so the default route aggregation needs to be turned off.

```
SWITCH(config)#router rip
SWITCH(config-router)#version 2
SWITCH(config-router)#passive-interface gigabitEthernet0/2
SWITCH(config-router)#no auto-summary
```

Associated Network

```
SWITCH(config-router)#network 10.10.1.0 255.255.255.0
SWITCH(config-router)#network 192.168.10.0 255.255.255.0
```

- Device S2 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.1.2/24
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 192.168.20.1/24
```

Configure the RIP process

Enable the rip process and configure the RIP version to version 2 so that routes with subnet masks can be advertised.

The internal network needs to learn specific subnet routes, so the default route aggregation needs to be turned off.

```
SWITCH(config)#router rip
SWITCH(config-router)#version 2
SWITCH(config-router)#no auto-summary
```

Associated Network

```
SWITCH(config-router)#network 10.10.1.0 255.255.255.0
SWITCH(config-router)#network 192.168.20.0 255.255.0.0
```

- Device S3 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.1.3/24
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 192.168.3.1/24
```

Configure the RIP process

Enable the rip process and configure the RIP version to version 2 so that routes with subnet masks can be advertised.

The internal network needs to learn specific subnet routes, so the default route aggregation needs to be turned off.

```
SWITCH(config)#router rip
SWITCH(config-router)#version 2
SWITCH(config-router)#no auto-summary
```

Associated Network

```
SWITCH(config-router)#network 10.10.1.0 255.255.255.0
SWITCH(config-router)#network 192.168.30.0 255.255.255.0
```

Configuring passive ports and specifying neighbors

In order to meet the requirement that S2 cannot learn the routes of S3, the S3 device needs to be configured with a passive interface, and the neighbor to learn the route must be S1

```
SWITCH(config-router)#passive-interface gigabitEthernet0/1
SWITCH(config-router)#neighbor 10.10.1.1
```

- Results display

Device S1：

The routing table is displayed on device S1, with routes from S2 and S3.

```
SWITCH#show ip route
```

```
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
C          192.168.10.0/24 is directly connected, gigabitEthernet0/2
R          192.168.20.0/24 [120/1] via 10.10.1.2, gigabitEthernet0/1, 02:50:16
R          192.168.30.0/24 [120/1] via 10.10.1.3, gigabitEthernet0/1, 02:51:29

Gateway of last resort is not set
SWITCH#
```

Device S2：

Display the routing table on device S2. Since S3 does not advertise routes to S2, it can be seen that there is no route advertised by S3

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
R          192.168.10.0/24 [120/1] via 10.10.1.1, gigabitEthernet0/1, 00:22:08
C          192.168.20.0/24 is directly connected, gigabitEthernet0/2

Gateway of last resort is not set
SWITCH#
```

Device S3：

Display the routing table on device S3, with routes from S1 and S2.

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
```

```
          * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
R          192.168.10.0/24 [120/1] via 10.10.1.1, gigabitEthernet0/1, 01:14:04
R          192.168.20.0/24 [120/1] via 10.10.1.2, gigabitEthernet0/1, 01:13:47
C          192.168.30.0/24 is directly connected, gigabitEthernet0/2
C          192.168.101.0/24 is directly connected, vlan100

Gateway of last resort is not set
SWITCH#
```

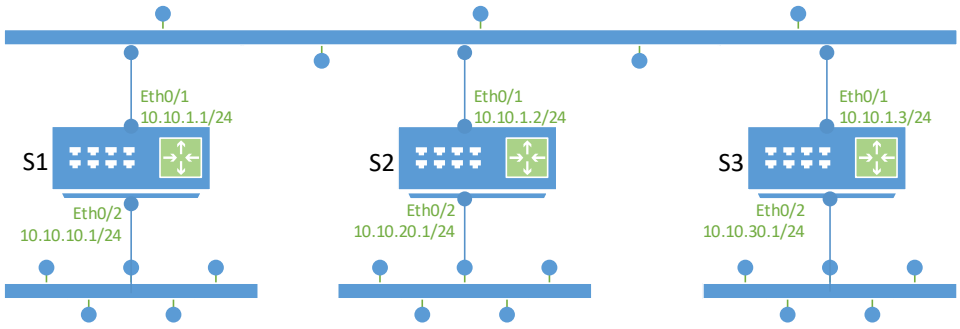
18.3.2.RIP default route configuration

Requirements

Three LAN switches S1, S2, S3:

- The three switches can learn routes from each other
- S2 advertises default routes to S1 and S3

Networking



Configure case

- Device S1 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.1.1/24
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
```

```
SWITCH(config-if)#ip address 10.10.10.1/24
```

Configure the RIP process

Enable the rip process and configure the RIP version to version 2 so that routes with subnet masks can be advertised.

Since the gigabitEthernet0/2 port of S1 is connected to the external network, in order to meet the requirement of receiving external network routes but not advertising routes to the external network, you need to configure the gigabitEthernet0/2 port as a passive interface.

The internal network needs to learn specific subnet routes, so the default route aggregation needs to be turned off.

```
SWITCH(config)#router rip
SWITCH(config-router)#version 2
SWITCH(config-router)#no auto-summary
```

Associated Network

```
SWITCH(config-router)#network 10.10.1.0 255.255.255.0
SWITCH(config-router)#network 10.10.10.0 255.255.255.0
```

- Device S2 configuration steps

Configure the ip address of port gigabitEthernet0/1, which is designated to advertise the default route, with a metric of 3

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.1.2/24
SWITCH(config-if)#ip rip default-information originate metric 3
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.20.1/24
```

Configure the RIP process

Enable the rip process and configure the RIP version to version 2 so that routes with subnet masks can be advertised.

The internal network needs to learn specific subnet routes, so the default route aggregation needs to be turned off.

```
SWITCH(config)#router rip
SWITCH(config-router)#version 2
SWITCH(config-router)#no auto-summary
```

Associated Network

```
SWITCH(config-router)#network 10.10.1.0 255.255.255.0
SWITCH(config-router)#network 10.10.20.0 255.255.255.0
```

- Device S3 configuration steps

Configure the ip address of port gigabitEthernet0/1

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.1.3/24
```

Configure the ip address of port gigabitEthernet0/2

```
SWITCH#configure terminal
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#no switchport
SWITCH(config-if)#ip address 10.10.30.1/24
```

Configure the RIP process

Enable the rip process and configure the RIP version to version 2 so that routes with subnet masks can be advertised.

The internal network needs to learn specific subnet routes, so the default route aggregation needs to be turned off.

```
SWITCH(config)#router rip
SWITCH(config-router)#version 2
SWITCH(config-router)#no auto-summary
```

Associated Network

```
SWITCH(config-router)#network 10.10.1.0 255.255.255.0
SWITCH(config-router)#network 10.10.30.0 255.255.255.0
```

- Results display

Device S1：

The routing table is displayed on device S1, with routes from S2 and S3.

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.10.1.2 to network 0.0.0.0

R*        0.0.0.0/0 [120/3] via 10.10.1.2, gigabitEthernet0/1, 00:00:38
```

```
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
C          10.10.10.0/24 is directly connected, gigabitEthernet0/2
R          10.10.20.0/24 [120/1] via 10.10.1.2, gigabitEthernet0/1, 00:11:08
R          10.10.30.0/24 [120/1] via 10.10.1.3, gigabitEthernet0/1, 00:10:27
SWITCH#
```

Device S2:

Display the routing table on device S2. Since S3 does not advertise routes to S2, it can be seen that there is no route advertised by S3

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
R          10.10.10.0/24 [120/2] via 10.10.1.1, gigabitEthernet0/1, 00:12:07
C          10.10.20.0/24 is directly connected, gigabitEthernet0/2
R          10.10.30.0/24 [120/1] via 10.10.1.3, gigabitEthernet0/1, 00:10:47

Gateway of last resort is not set
SWITCH#
```

Device S3:

Display the routing table on device S3, with routes from S1 and S2.

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.10.1.2 to network 0.0.0.0

R*         0.0.0.0/0 [120/1] via 10.10.1.2, gigabitEthernet0/1, 00:03:06
C          10.10.1.0/24 is directly connected, gigabitEthernet0/1
R          10.10.10.0/24 [120/1] via 10.10.1.1, gigabitEthernet0/1, 00:01:18
R          10.10.20.0/24 [120/1] via 10.10.1.2, gigabitEthernet0/1, 00:07:56
```

```
C          10.10.30.0/24 is directly connected, gigabitEthernet0/2
SWITCH#
```

18.4. DISPLAY COMMAND

- Display routing information

```
SWITCH#show ip route
Codes: K - kernel, C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 10.10.1.2 to network 0.0.0.0

R*        0.0.0.0/0 [120/1] via 10.10.1.2, gigabitEthernet0/1, 00:03:06
C         10.10.1.0/24 is directly connected, gigabitEthernet0/1
R         10.10.10.0/24 [120/1] via 10.10.1.1, gigabitEthernet0/1, 00:01:18
R         10.10.20.0/24 [120/1] via 10.10.1.2, gigabitEthernet0/1, 00:07:56
C         10.10.30.0/24 is directly connected, gigabitEthernet0/2
SWITCH#
```

- Only display RIP routing information

```
SWITCH#show ip route rip
IP Route Table for VRF "default"
R         10.10.30.0/24 [120/1] via 10.10.1.3, gigabitEthernet0/1, 00:44:29
R         192.168.101.0/24 [120/1] via 10.10.1.3, gigabitEthernet0/1, 00:44:29

Gateway of last resort is not set
SWITCH#
```

- Other RIP information

Command	Function
show ip rip database	Dispaly RIP database
show ip rip external	Display RIP republished routing information
show ip rip interface	Display RIP-related interface information
show ip rip peer	Display RIP peer information

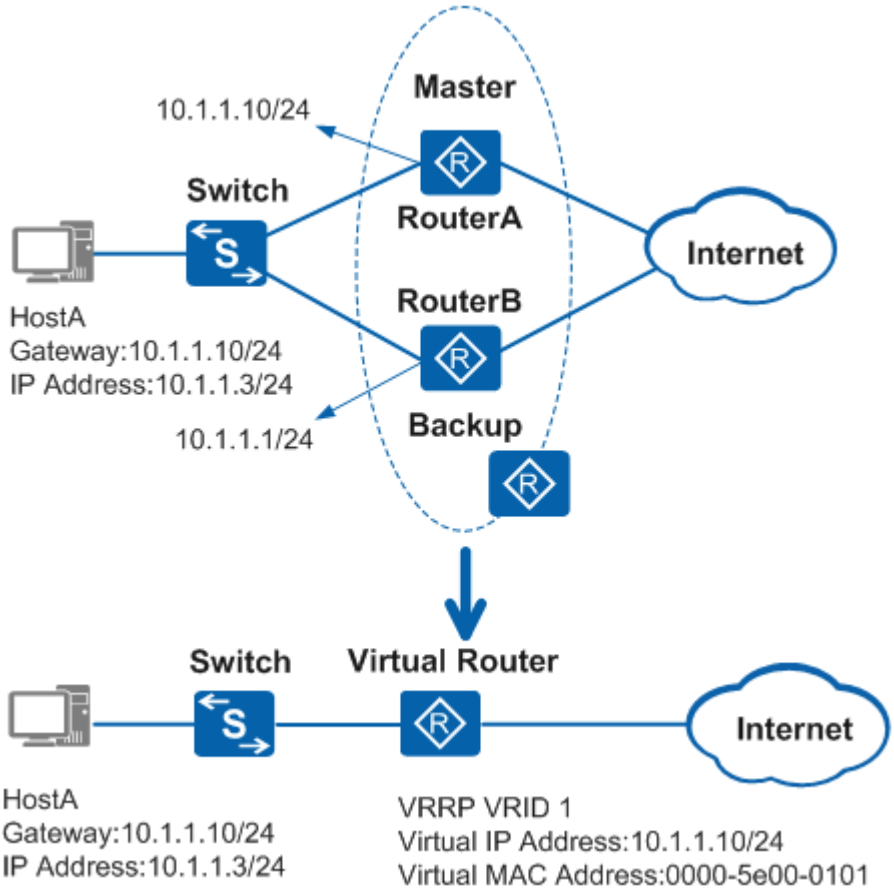
19. CONFIGURE VRRP

19.1. PROTOCOL OVERVIEW

Virtual Router Redundancy Protocol (VRRP) combines several routing devices to form a virtual routing device, and uses the IP address of the virtual routing device as the user's default gateway to communicate with the external network. When a gateway device fails, the VRRP mechanism can elect a new gateway device to undertake data traffic, thereby ensuring reliable network communication.

This device only supports VRRPv2 function.

Networking topology



Definition of Terms

- VRRP Router: A device running the VRRP protocol, which may belong to one or more virtual routers, such as RouterA and RouterB.

- Virtual Router: Also known as VRRP backup group, it consists of a Master device and multiple Backup devices, and is used as the default gateway for hosts in a shared LAN. For example, RouterA and RouterB together form a virtual router.
- Master router (Virtual Router Master): VRRP device that undertakes the task of forwarding packets, such as RouterA.
- Backup router (Virtual Router Backup): A group of VRRP devices that do not undertake forwarding tasks. When the master device fails, they will become the new master device through election, such as RouterB.
- VRID: The ID of the virtual router. For example, the VRID of the virtual router composed of RouterA and RouterB is 1.
- Virtual IP Address: The IP address of the virtual router. A virtual router can have one or more IP addresses, which are configured by the user. For example, the virtual IP address of the virtual router composed of RouterA and RouterB is 10.1.1.10/24.
- IP Address Owner: If a VRRP device uses the virtual router IP address as the real interface address, the device is called the IP address owner. If the IP address owner is available, it will usually become the Master. For example, RouterA has the same IP address as that of the virtual router, 10.1.1.10/24. Therefore, it is the owner of the IP address of this VRRP backup group.
- Virtual MAC Address: The MAC address generated by the virtual router according to the virtual router ID. A virtual router has a virtual MAC address in the format: 00-00-5E-00-01-{VRID}(VRRP for IPv4); 00-00-5E-00-02-{VRID}(VRRP for IPv6). When the virtual router responds to ARP requests, the virtual MAC address is used instead of the real MAC address of the interface. For example, the VRID of the virtual router composed of RouterA and RouterB is 1, so the MAC address of this VRRP backup group is 00-00-5E-00-01-01.

19.2. CONFIG. COMMAND

- Create /delete VRRPgroup

Command	SWITCH(config)# **vrrp router** <1-255> SWITCH(config)#**no vrrp router** <1-255>
Decription	Global configuration mode . Create /delete a VRRP group.

- Associated VRRP port

Command	SWITCH(config-vrrp)#**interface** IFNAME SWITCH(config-vrrp)#**no interface**
Description	VRRP group configuration mode. Configure/delete the Layer 3 interface associated with the VRRP group. Supports SVI ports, such as vlan1; does not support Layer 2 ports, such as gigabitEthernet0/1 that is not configured as a Layer 3 port.

- Configure/delete VRRP virtual address

Command	SWITCH(config-vrrp)#**virtual-ip** A.B.C.D {master|backup} SWITCH(config-vrrp)#**no virtual-ip**
Description	VRRP group configuration mode. The virtual address is the virtual router gateway address. Configured as the master role must ensure that the virtual IP is the interface IP associated with the group.

- Configure enable/disable VRRP group

Command	SWITCH(config-vrrp)#**enable** SWITCH(config-vrrp)#**no enable**
Description	VRRP group configuration mode. Before enabling a VRRP group, you must configure the associated interface and virtual address.

- Configure/delete VRRP priority

Command	SWITCH(config-vrrp)#**priority** <1-255> SWITCH(config-vrrp)#**no priority**
Description	VRRP group configuration mode. Optional. A priority of 0 is reserved by the system for special use; a priority value of 255 is reserved for the IP address owner. By default, the priority value of the backup router is 100. The higher the value, the higher the priority.

- Configure/reset VRRP group advertisement interval

Command	SWITCH(config-vrrp)#**advertisement-interval** <1-10> SWITCH(config-vrrp)#**no advertisement-interval**

Description	VRRP group configuration mode. Optional configuration, the unit is seconds, the default is 1.

- Configure/delete preemptive mode

Command	SWITCH(config-vrrp)#**preempt-mode on** SWITCH(config-vrrp)#**no preempt-mode**
Description	VRRP group configuration mode. Optional configuration, preemption is enabled by default.

- Configure the authentication function

Command	SWITCH(config-vrrp)#**authentication text** LINE SWITCH(config-vrrp)#**no authentication**
Description	VRRP group configuration mode. Optional configuration, default authentication-free mode. VRRPv1 supports authentication-free mode, simple key authentication mode, and md5 authentication mode, but does not improve security; VRRPv2 is compatible with v1 authentication mode; VRRPv3 cancels the security field. It is not recommended to configure the authentication function on the device.

- Configure line failover

Command	SWITCH(config-vrrp)#**circuit-failover** IFNAME <1-253> SWITCH(config-vrrp)#**no circuit-failover**
Description	VRRP group configuration mode. Optional configuration, the line failover function is not enabled by default. After the configuration, the VRRP group will monitor the configured lines. Once a line failure is found, it will adjust the configured priority offset to realize the re-election of the protocol.

19.3. CONFIG.CASE

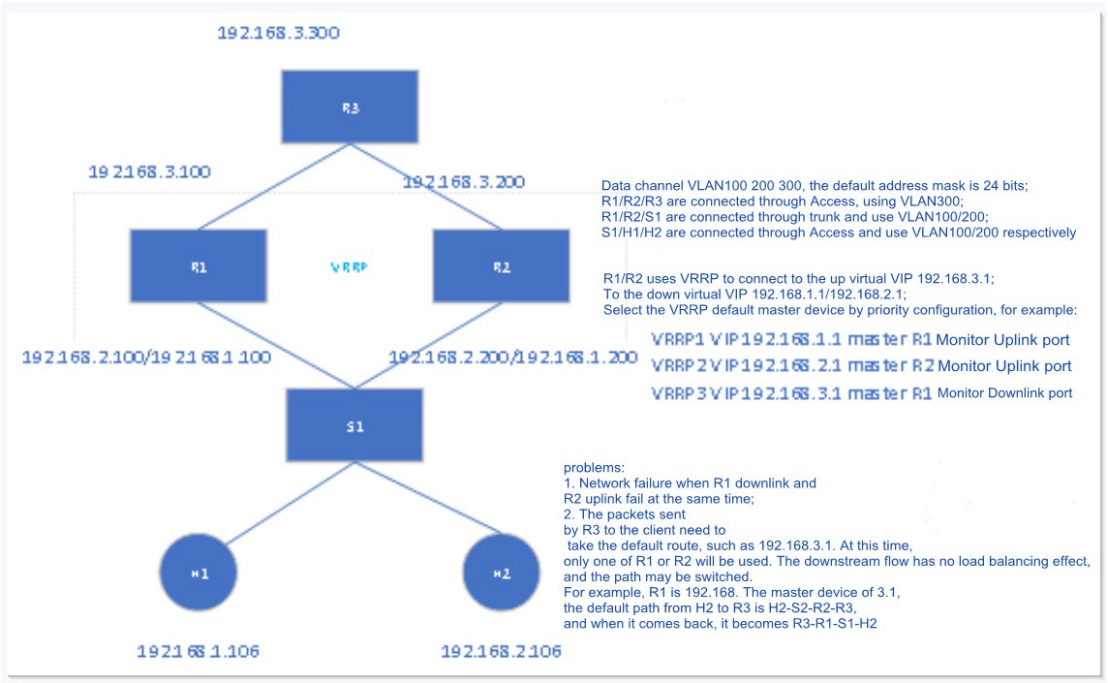
19.3.1. Load Balancing Scenario

Requirements

- Under normal circumstances, the dual gateways share user traffic equally.
- □ When the gateway device is faulty, users can still access the external network.

Networking dia.

Dia. 21-1 VRRP Load balancing networking diagram



Typical configuration Eg.

R3:

```
SWITCH(config)# vlan 300
SWITCH(config)#interface vlan300
SWITCH(config-if)# ip address 192.168.3.300/24
SWITCH(config)# ip route 0.0.0.0 0.0.0.0 192.168.3.1
```

R1:

```
SWITCH(config)# vlan 100,200,300
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)# switchport access vlan 300
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)# switchport mode trunk
SWITCH(config-if)# switchport trunk allow-vlan 100,200
SWITCH(config)#interface vlan100
SWITCH(config-if)# ip address 192.168.1.100/24
SWITCH(config)#interface vlan200
SWITCH(config-if)# ip address 192.168.2.100/24
SWITCH(config)#interface vlan300
SWITCH(config-if)# ip address 192.168.3.100/24
SWITCH(config)# vrrp router 1
SWITCH(config-vrrp)# interface vlan100
SWITCH(config-vrrp)# virtual-ip 192.168.1.1 backup
SWITCH(config-vrrp)# circuit-failover vlan300
```

```
SWITCH(config-vrrp)# enable
SWITCH(config)# vrrp router 2
SWITCH(config-vrrp)# interface vlan200
SWITCH(config-vrrp)# virtual-ip 192.168.2.1 backup
SWITCH(config-vrrp)# circuit-failover vlan300
SWITCH(config-vrrp)# priority 90
SWITCH(config-vrrp)# enable
SWITCH(config)# vrrp router 3
SWITCH(config-vrrp)# interface vlan300
SWITCH(config-vrrp)# virtual-ip 192.168.3.1 backup
SWITCH(config-vrrp)# circuit-failover gigabitEthernet0/10
SWITCH(config-vrrp)# enable
```

R2:

```
SWITCH(config)# vlan 100,200,300
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)# switchport access vlan 300
SWITCH(config)#interface gigabitEthernet0/10
SWITCH(config-if)# switchport mode trunk
SWITCH(config-if)# switchport trunk allow-vlan 100,200
SWITCH(config)#interface vlan100
SWITCH(config-if)# ip address 192.168.1.200/24
SWITCH(config)#interface vlan200
SWITCH(config-if)# ip address 192.168.2.200/24
SWITCH(config)#interface vlan300
SWITCH(config-if)# ip address 192.168.3.200/24
SWITCH(config)# vrrp router 1
SWITCH(config-vrrp)# interface vlan100
SWITCH(config-vrrp)# virtual-ip 192.168.1.1 backup
SWITCH(config-vrrp)# circuit-failover vlan300
SWITCH(config-vrrp)# priority 90
SWITCH(config-vrrp)# enable
SWITCH(config)# vrrp router 2
SWITCH(config-vrrp)# interface vlan200
SWITCH(config-vrrp)# virtual-ip 192.168.2.1 backup
SWITCH(config-vrrp)# circuit-failover vlan300
SWITCH(config-vrrp)# enable
SWITCH(config)# vrrp router 3
SWITCH(config-vrrp)# interface vlan300
SWITCH(config-vrrp)# virtual-ip 192.168.3.1 backup
SWITCH(config-vrrp)# circuit-failover gigabitEthernet0/10
SWITCH(config-vrrp)# priority 90
```

```
SWITCH(config-vrrp)# enable
```

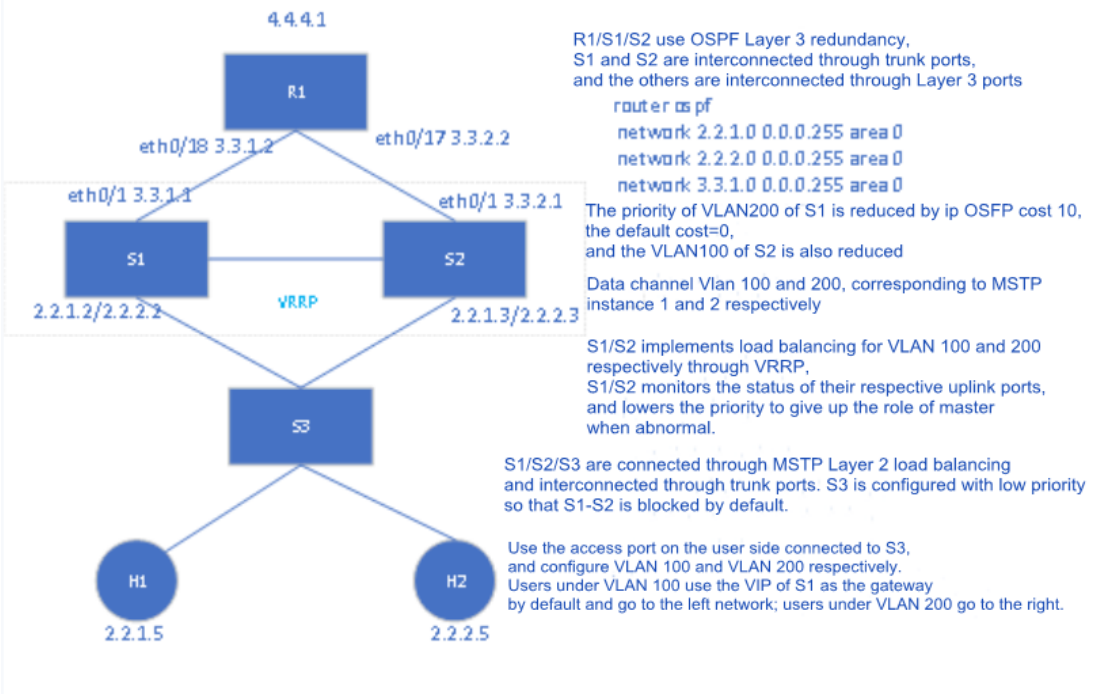
19.3.1. MSTP+VRRP+OSPF scenes

Requirements

- Under normal circumstances, the dual gateways share user traffic equally.
- When the gateway device is faulty, users can still access the external network.
- When two uplink and downlink links fail at the same time, users can still access the external network

Networking

Dia. 21-2 MSTP+VRRP networking dia.



Typical configuration E.g.

S3.txt S2.txt S1.txt R1.txt

19.4. DISPLAY COMMAND

- DISPLAY vrrp group information

```
#show vrrp
```

```
---------------- VRRP 1 ----------------
ID:                     1
State:                  Master (Enabled)
Virtual IP:             2.2.1.1/24 (Not IP owner)
Last Master:            2.2.1.3 (63510s ago)
Interface:              vlan100
Priority:               100 (conf.-1)
Advertisement interval: 1 sec
Preempt mode:           TRUE
Authentication:         none
---------------- VRRP 2 ----------------
ID:                     2
State:                  Backup (Enabled)
Virtual IP:             2.2.2.1/24 (Not IP owner)
Last Master:            2.2.2.3 (0s ago)
Interface:              vlan200
Priority:               90 (conf.90)
Advertisement interval: 1 sec
Preempt mode:           TRUE
Authentication:         none
```

20. CONFIG. ACL

20.1. ACL OVERVIEW

An ACL (Access Control List) implements packet filtering by configuring matching rules and processing operations for packets. It can effectively prevent illegal users from accessing the network, and can also control traffic and save network resources.

Packet matching rules defined by ACL can also be referenced by other functions that need to differentiate traffic, such as the definition of traffic classification rules in QoS.

ACL classifies packets through a series of matching conditions, which can be SMAC, DMAC, SIP, DIP, etc. of the packet. According to the matching conditions, ACLs can be divided into the following types:

Standard IP-based ACL: Make rules based only on the source IP address of the packet.

IP-based extended ACL: formulate rules based on the source IP address, destination IP address, ETYPE, and protocol of the data packet.

MAC-based ACL: Formulate rules based on the source MAC address and destination MAC address of the data packet.

Nameable ACL: formulating rules are the same as IP-based standard ACL and extended ACL.

20.2. CONFIG.COMMAND

- Configure IP-based standard ACL

Command	SWITCH(config)#**ip-access-list** {<1-99> | <1300-1999>} {**permit | deny**} {SIPADDR SIPADDRMASK | **any**} SWITCH(config)#**no ip-access-list** {<1-99> | <1300-1999>} {**permit | deny**} {SIPADDR SIPADDRMASK | **any**} SWITCH(config)#**no ip-access-list** {<1-99> | <1300-1999>}
Description	Create/Delete IP-based Standard ACLs

- Configure IP-based extended ACL

Command	SWITCH(config)# **ip-access-list** {<100-199> | <2000-2699>} {**permit | deny**} {TYPE} {SIPADDR SIPADDRMASK | **any**} {DIPADDR DIPADDRMASK | **any**} SWITCH(config)#**no ip-access-list** {<100-199> | <2000-2699>} {**permit | deny**} TYPE {SIPADDR SIPADDRMASK | **any**} {DIPADDR DIPADDRMASK | **any**} SWITCH(config)# **no ip-access-list** {<100-199> | <2000-2699>}
Description	Create/Delete IP-based Extended ACL TYPE lists ：

	<0-255>: Specifies the ID of the protocol any: any protocol packets gre: GRE packets IGMP: IGMP packets IP: IPv4 packets ipcomp: IPComp packets ospf: OSPF packets pim: PIM packets rsvp: RSVP packets tcp: TCP packets udp: UDP packets vrrp: VRRP packets

- Configure MAC-based ACL

Command	SWITCH(config)#**mac-access-list** <200-699> {**permit** **| deny**} {SMAC SMACMASK	**any**} {DMAC DMACMASK	**any**} SWITCH(config)#**no mac-access-list** <200-699> {**permit** **| deny**} {SMAC SMACMASK	**any**} {DMAC DMACMASK	**any**} SWITCH(config)#**no mac-access-list** <200-699>
Description	Create/Delete MAC-based ACLs

- Configure standard IP nameable ACL

Command	SWITCH(config)#**ip-access-list standard** ACLNAME {**permit** **| deny**} {SIPADDR SIPADDRMASK	**any**} SWITCH(config)#**no ip-access-list standard** ACLNAME {**permit** **| deny**} {SIPADDR SIPADDRMASK	**any**} SWITCH(config)#**no ip-access-list standard** ACLNAME
Descrption	Create/Delete Standard IP Nameable ACL

- Configure extended IP nameable ACL

Command	SWITCH(config)#**ip-access-list extended** ACLNAME {**permit** **| deny**} TYPE {SIPADDR SIPADDRMASK	**any**} {DIPADDR DIPADDRMASK	**any**} SWITCH(config)#**no ip-access-list extended** ACLNAME {**permit** **| deny**} TYPE {SIPADDR SIPADDRMASK	**any**} {DIPADDR DIPADDRMASK	**any**} SWITCH(config)#**no ip-access-list extended** ACLNAME
Description	Create/Delete Extended IP Nameable ACL

Illustration

✦ A maximum of 128 rules can be configured under a single ACL-ID;

✦ Invert the mask, such as matching IP addresses in the 192.168.1.0/24 range, configure 192.168.1.0 0.0.0.255;

✦ The name of the ACL can be named, the first character cannot be a number;

✦ MAC-based ACL does not take effect on IP and ARP packets;

- Configure the ACL to be applied to the port

Command	SWITCH(config-if)#**access-group** ACLNAME **input** SWITCH(config-if)#**no access-group** ACLNAME **input**
Description	Configure/delete ACL applied on port

Illustration

✦ When an ACL has been applied to a port, if you need to add or delete rules, you must first de-apply it from the port;

20.3. CONFIG. E.G.

Case 1: Filter the ingress packets of port gigabitEthernet0/1, allow the packets whose SIP is 192.168.1.0/24, and discard other packets.

- Configure ACL rules:

```
SWITCH(config)#ip-access-list 1  permit  192.168.1.0 0.0.0.255
SWITCH(config)#ip-access-list 1 deny any
```

- Apply ACL to port gigabitEthernet0/1

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#access-group 1 in
```

20.4. DISPALY COMMAND

- Display ACL

```
SWITCH#show ip-access-list 1
  Standard IP access list: 1
    permit 1.1.1.1
    deny   any
```

```
SWITCH#show mac-access-list 200
  Extended MAC-ACCESS-LIST: 200
    permit host 0001.0002.0003 any
deny   any any
```

21. CONFIG. QOS

21.1. QOS OVERVIEW

QoS (Quality of Service, quality of service) refers to a network can use various basic technologies to provide better service capabilities for specified network communications.

The traditional network adopts a "best effort" forwarding mechanism. When the network bandwidth is abundant, all data flows are handled well. When the network is congested, all data flows may be discarded. In order to meet the requirements of different quality of service of different applications, it is required that the network can allocate and schedule resources according to the requirements of users, and provide different quality of service for different data streams.

A device that supports the QoS function can provide transmission quality services. For a certain type of data flow, it can be given a certain level of transmission priority to identify its relative importance, and use the various priorities provided by the device. Mechanisms such as forwarding strategies and congestion avoidance provide special transmission services for these data streams.

The network environment configured with QoS increases the predictability of network performance, and can effectively allocate network bandwidth and utilize network resources more reasonably.

21.2. CONFIG.COMMAND

- Globally enable/disable QOS

Command	SWITCH(config)#**mls qos enable** SWITCH(config)#**no mls qos**
Descrption	Globally enable and disable the QOS function Off by default

- Configure the queue scheduling algorithm

Command	SWITCH(config)#**mls qos algorithm** {**sp** | **wrr**}
Description	Configure the queue scheduling algorithm, support 2 modes: wrr (balanced scheduling), sp (absolute scheduling) Default is wrr mode

- Configure queue weight

Command	SWITCH(config)#**mls qos wrr-weight** <0-7> <0-32>

Description	Configure the queue weight. The queue weight is only valid for wrr mode The default weight of all queues is 1 When in wrr mode, configure the queue weight as 0, the queue scheduling weight is infinite

- Configure port trust mode

Conmmand	SWITCH(config-if)#**mls qos trust** {**cos | dscp**} SWITCH(config-if)#**no mls qos trust**
Description	Configure the port trust mode, the default is not trust When in no trust mode, the entry stage modifies the cos field and dscp field of the message according to the default cos of the port; when trust cos is configured, the same as the no trust mode for untagged messages, and for tagged messages, choose the message with its own cos; When configuring trust dscp, for ip packets, select the packet with dscp, and for non-ip packets, it is the same as trust cos mode.

- Configure port default cos

Command	SWITCH(config-if)#**mls qos cos** <0-7> SWITCH(config-if)#**no mls qos cos**
Description	Configure the default cos of the port. The default cos takes effect for the ingress port without tags. The default port cos is 0

- Configure the cos-dscp mapping relationship

Command	SWITCH(config)#**mls qos cos-dscp** <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> <0-63> SWITCH(config)#**no mls qos cos-dscp**
Description	Configure/delete cos-dscp mapping relationship Default cos-dscp mapping relationship：0-0，1-8，2-16，3-24，4-32，5-40，6-48，7-56

- Configure the cos-queue mapping relationship

Command	SWITCH(config)#**mls qos cos-queue** <0-7> <0-7> SWITCH(config)#**no mls qos cos-queue** <0-7>
Description	Configure/delete cos-queue mapping relationship Default cos-dscp mapping relationship：0-0，1-1，2-2，3-3，4-4，5-5，6-6，7-7

Illustration

✦ When the configured port is no trust, trust cos, or trust dscp and is not an ip packet: the cos-dscp configuration takes effect, modify the packet dscp according to the mapping relationship, and the cos-queue configuration takes effect, and modify the packet export queue according to the mapping relationship;

- Configure the dscp-cos mapping relationship

Command	SWITCH(config)#**mls qos dscp-cos** <0-63> to <0-7> SWITCH(config)#**no mls qos dscp-cos**
Description	Configure the dscp-cos mapping relationship Default cos-dscp mapping relationship：<0-7>-0，<8-15>-1，<16-23>-2，<24-31>-3，<32-39>-4，<40-47>-5，<48-55>-6，<56-63>-7

- Configure the dscp-dscp mapping relationship

Command	SWITCH(config)#**mls qos dscp-mutation** <0-63> to <0-63> SWITCH(config)#**no mls qos dscp-mutation**
Description	Configure the dscp-dscp mapping relationship

- Configure the dscp-queue mapping relationship

Command	SWITCH(config)#**mls qos dscp-queue** <0-63> <0-7> SWITCH(config)#**no mls qos dscp-queue** <0-63>
Description	Configure the dscp-queue mapping relationship

	Default dscp-queue mapping relationship：<0-7>-0，<8-15>-1，<16-23>-2，<24-31>-3，<32-39>-4，<40-47>-5，<48-55>-6，<56-63>-7

Illustration

✦ When configuring the port as trust dscp and ip packets: the dscp-cos configuration takes effect, modify the packet dscp according to the mapping relationship, and the dscp-queue configuration takes effect, and modify the packet egress queue according to the mapping relationship. When a colleague configures dscp-dscp at the same time, first perform dscp-dscp conversion, and then perform dscp-cos mapping;

- Configure class-map

Command	SWITCH(config)#**class-map** CNAME SWITCH(config-cmap)# SWITCH(config)#**no class-map** CNAME
Description	Create /delete class-map After creating class-map，enter class-mapmode automatically

- Configure flow matching rules

Command	SWITCH(config-cmap)# **match access-group** ACLNAME SWITCH(config-cmap)#**no match access-group** ACLNAME
Description	Configure ACL-based chassis-map, support standard IP, extended IP, and MAC ACL

Command	SWITCH(config-cmap)#**match ip-dscp** <0-63> SWITCH(config-cmap)#**no match ip-dscp**
Description	Configure to match the dhcp field in the IP packet, up to 8 different dhcp values can be configured

Command	SWITCH(config-cmap)#**match cos** <0-7> SWITCH(config-cmap)#**no match cos**
Description	Configure the cos field in the matching message, up to 8 different cos values can be configured

Command	SWITCH(config-cmap)#**match ethertype** ETYPE SWITCH(config-cmap)#**no match ethertype**

Description	Match the Ethernet protocol type field of the packet

Command	SWITCH(config-cmap)#**match** {**vlan** <1-4094> | **vlan-range** <1-4094> **to** <1-4094>} SWITCH(config-cmap)**#no match** {**vlan | vlan-range**}
Description	Match packet vlan, support range configuration

Command	SWITCH(config-cmap)#**match layer4** {**tcp | udp**} {**source-port | destination-port**} VALUE SWITCH(config-cmap)#**no match layer4** {**tcp | udp**} {**source-port | destination-port**} VALUE
Description	Support IPv4 protocol packet Layer 4 port number configuration

Command	SWITCH(config-cmap)#**match vlan-range** <1-4094> to <1-4094> **ethertype** ETYPE SWITCH(config-cmap)#**no match vlan-range**
Description	Match packet vlan, support range configuration, and match packet etype

- Configure policy-map

Command	SWITCH(config)#**policy-map** PNAME SWITCH(config-pmap)# SWITCH(config)#**no policy-map** PNAME
Description	Create /delete policy-map

- Configure policy-map to associate class-map

Command	SWITCH(config-pmap)# **class-map** CNAME SWITCH(config-pmap-c)# SWITCH(config-pmap)#**no class-map** CNAME
Description	policy-map association/disassociation class-map A policy-map can attach up to 8 class-maps

- Configuration strategy

Command	SWITCH(config-pmap-c)#**set cos** <0-7> SWITCH(config-pmap-c)#**no set cos**
Description	Configure/delete policies and modify the cos field of packets

Command	SWITCH(config-pmap-c)#**set ip-dscp** <0-63> SWITCH(config-pmap-c)#**no set ip-dscp**
Description	Configure/delete policies and modify the ip-dscp field of packets

Command	SWITCH(config-pmap-c)#**set vlan** <1-4094> SWITCH(config-pmap-c)#**no set vlan**
Description	Configure/delete policies, modify packet vlan

Command	SWITCH(config-pmap-c)#**nest vlan** <1-4094> SWITCH(config-pmap-c)#**no nest vlan**
Description	Configure/delete policies and add external tags to matching packets

Command	SWITCH(config-pmap-c)#**police cir** <32-1000000> **cbs** <4-31250> **exceed-action drop** SWITCH(config-pmap-c)#**no police**
Description	Configure/Delete Policy Cir is the speed limit water line, in kbps Cbs is burst capacity, unit Kbyte

Illustration

✦ The value of cir is determinable. For example, if the speed limit is 1M, then the value of cir is 1024, but the value of cbs is taken from the empirical value. When the cbs value is set large, the flow peak is higher and the speed limit is more stable, but the average speed may be higher than the speed limit value; when the cbs value is small, the flow peak is lower, the speed limit fluctuates greatly, and the average speed may be lower than the speed limit value . It is recommended that the cbs configuration be 4 times the value of cir and a small value of 31250.

- Configure the policy-map to be applied on the interface

Command	SWITCH(config-if)#**service-policy input** PNAME SWITCH(config-if)#**no service-policy input**

Description	Configure/delete the application of the policy on the interface Only one policy-map can be applied to an interface

- Configure port ingress rate limit

Command	SWITCH(config-if)#**rate-limit input** <64-1000000> <32-16384> SWITCH(config-if)#**no rate-limit input**
Description	Configure/delete port ingress rate limit The first parameter is limit, in kbps The second parameter is burst, the unit is Kbyte

- Configure port ingress and egress rate limit

Command	SWITCH(config-if)#**rate-limit output** <64-1000000> <32-16384> SWITCH(config-if)#**no service-policy output**
Description	Configure/delete port egress rate limit The first parameter is limit, in kbps The second parameter is burst, the unit is Kbyte

Illustration

✦ The limit value is determinable. For example, if the speed limit is 1M, then the limit value is 1024, but the burst value is taken from the experience value. When the burst value is large, the flow peak is higher, and the speed limit is stable, but the average rate may be higher than the speed limit value; when the burst value is small, the flow peak is lower, the speed limit fluctuates greatly, and the average rate may be lower than the speed limit value. . It is recommended that the burst configuration be 4 times the limit value and a small value of 16384.

21.3. CONFIGURE CASE:

Case 1: The ingress speed limit is 1024kbps for port gigabitEthernet0/1, and the egress speed limit is 1024kbps.

- Configure gigabitEthernet0/1 ingress rate limit:

```
SWITCH(config-if)#rate-limit input 1024 4096
```

- Configure gigabitEthernet0/1 export speed limit:

```
SWITCH(config-if)#rate-limit output 1024 4096
```

Case 2: The ingress rate is limited to 1024kbps for the flow whose SIP is 192.168.64.1 on port gigabitEthernet0/1.

- Configure the global open QOS function:

```
SWITCH(config)#mls qos enable
```

- Create ACL flow:

```
SWITCH(config)#ip-access-list 1 permit 192.168.64.1
```

- Configure class-map、policy-map:

```
SWITCH(config)#class-map c1
SWITCH(config-cmap)#match access-group 1
SWITCH(config-cmap)#exit
SWITCH(config)#policy-map p1
SWITCH(config-pmap)#class-map c1
SWITCH(config-pmap-c)#police cir 1024 cbs 4096 exceed-action drop
```

- Configure the port application policy-map:

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#service-policy input p1
```

Case 3: When the network is congested, it is required that the entry of gigabitEthernet0/2 does not carry tags to be forwarded preferentially

- Configure the global open QOS function:

```
SWITCH(config)#mls qos enable
```

- The default cos of the port configured on gigabitEthernet0/2 is 2, the port trusts the cos, the default cos of the port configured on gigabitEthernet0/1 is 0, and the cos is trusted:

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#mls qos trust cos
SWITCH(config-if)#mls qos cos 0
SWITCH(config-if)#exit
SWITCH(config)#interface gigabitEthernet0/2
SWITCH(config-if)#mls qos trust cos
SWITCH(config-if)#mls qos cos 2
```

- Configure the cos-queue queue mapping relationship:

```
SWITCH(config)#mls qos cos-queue 0 0
SWITCH(config)#mls qos cos-queue 2 2
```

- Configure the scheduling mode to wrr:

```
SWITCH(config)#mls qos algorithm wrr
```

- Configure the weight of queue 2 to 0:

```
SWITCH(config)#mls qos weight 2 0
```

21.4. DISPLAY COMMAND

- Display scheduling mode, weight configuration information

```
SWITCH#show mls qos algorithm
Mls qos algorithm is WRR.

Queue-id    0     1     2     3     4     5     6     7
Weight      1     1     1     1     1     1     1     1
```

- Display cos-map configuration information

```
SWITCH#show mls qos cos-maps
----------------------------
Cos       Dscp       Queue
----------------------------
0         0          0
1         8          1
2         16         2
3         24         3
4         32         4
5         40         5
6         48         6
7         56         7
```

- Display dscp-map configuration information

```
SWITCH#show mls qos dscp-maps
-----------------------------------------
Dscp       Cos       Mutation       Queue
-----------------------------------------
0          0         0                 0
1          0         1                 0
2          0         2                 0
3          0         3                 0
4          0         4                 0
5          0         5                 0
6          0         6                 0
7          0         7                 0
8          1         8                 1
9          1         9                 1
10         1         10                1
11         1         11                1
12         1         12                1
13         1         13                1
14         1         14                1
15         1         15                1
```

- Display interface configuration information

```
SWITCH#show mls qos interfaces
```

```
-------------------------------
Interface     Trust mode  Cos
-------------------------------
GiE0/1        Not         0
GiE0/2        Not         0
GiE0/3        Not         0
GiE0/4        Not         0
GiE0/5        Not         0
GiE0/6        Not         0
GiE0/7        Not         0
GiE0/8        Not         0
GiE0/9        Not         0
GiE0/10       Not         0
```

- Display class-map configuration information

```
SWITCH#show class-map

    CLASS-MAP-NAME: c1
      Match Cos: 3
```

- Display policy-map configuration information

```
SWITCH#show policy-map

  POLICY-MAP-NAME: p1
    State: detached

    CLASS-MAP-NAME: c1
      Match Cos: 3
      Police: Mode: SrTCM
              cir (1024 Kbps)
              cbs (4096 KBytes)
              exceed-action (drop)
```

- Display port rate limit configuration information

```
SWITCH#show rate-limit
-----------------------------------------------------------
Interface     In limit  In burst  Out limit  Out burst
-----------------------------------------------------------
GiE0/1        --        --        --         --
GiE0/2        --        --        --         --
GiE0/3        1024      4096      --         --
GiE0/4        --        --        --         --
GiE0/5        --        --        --         --
GiE0/6        --        --        --         --
```

GiE0/7	--	--	--	--
GiE0/8	--	--	--	--
GiE0/9	--	--	--	--
GiE0/10	--	--	1024	4096

22. CONFIGURE DHCP SNOOPING

22.1. DHCP SNOOPING OVERVIEW

DHCP (Dynamic Host Configuration Protocol, Dynamic Host Configuration Protocol) is a network protocol of a local area network, which is widely used to dynamically allocate reusable network resources. It is a means for users or internal network administrators to centrally manage all computers. DHCP Snooping is a DHCP security technology that isolates illegal DHCP servers by detecting and managing DHCP exchange messages. DHCP Snooping divides ports into two types: TRUST port and UNTRUST port. The device only forwards DHCP Offer messages received by the TRUST port, and discards all DHCP Offer messages from the UNTRUST port, thereby shielding illegal DHCP servers.

22.2. CONFIGURE COMMAND

- Globally enable/disable DHCP Snooping

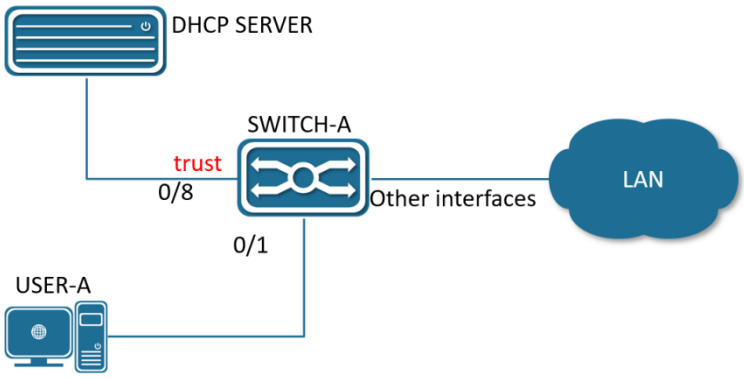
Command	SWITCH(config)#**ip dhcp snooping** SWITCH(config)#**no ip dhcp snooping**
Description	Globally enable and disable DHCP Snooping

- Configure the trusted port

Command	OLT(config-if)#**ip dhcp snooping trust** OLT(config-if)#**no ip dhcp snooping trust**
Description	Set the port to TRUST/UNTRUST port

22.3. CONFIGURE CASE

Case 1: For SWITCH-A, the gigabitEthernet0/8 interface is connected to the DHCP server, and USER-A obtains the IP address dynamically. The existence of other DHCP servers in the LAN will affect the IP address assignment of USER-A.



- Enter the global mode and enable the DHCP Snooping function globally:

```
SWITCH#configure terminal
SWITCH(config)#ip dhcp snooping
```

- Configure the uplink port gigabitEthernet0/8 connected to the server as a trusted port

```
SWITCH(config)#interface gigabitEthernet0/8
SWITCH(config-if)#ip dhcp snooping trust
```

22.4. DISPLAY COMMAND

- Display DHCP Snooping configuration information

```
SWITCH#show ip dhcp snooping
IP DHCP Snooping status: Enabled

Interface          TRUSTED
---------------------------
GiE0/1             NO
GiE0/2             NO
GiE0/3             NO
GiE0/4             NO
GiE0/5             NO
GiE0/6             NO
GiE0/7             NO
GiE0/8             YES
GiE0/9             NO
GiE0/10            NO
```

23. CONFIGURE 802.1X AUTHENTICATION

23.1. PROTOCOL OVERVIEW

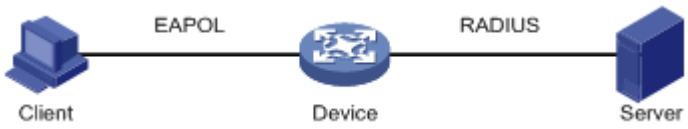
The IEEE802 LAN/WAN committee proposed the 802.1X protocol to solve the problem of wireless local area network network security. Later, 802.1X protocol was widely used in Ethernet as a common access control mechanism of LAN port, mainly to solve the problems of authentication and security in Ethernet.

The 802.1X protocol is a port based network access control protocol. "Port-based network access control" means that, at the level of the port of the LAN access device, the access to the network resources is controlled through authentication for the accessed user equipment.

23.1.1.802.1X Architecture

The 802.1X system is a typical Client/Server structure, as shown in Figure 1-1, including three entities: the client (Client), the device (Device) and the authentication server (Server).

Figure 1-1 Architecture of 802.1X Authentication System



- The client is an entity located at one end of the LAN segment, which is authenticated by the device at the other end of the link. The client is generally a user terminal device, and the user can initiate 802.1X authentication by starting the client software. Clients must support EAPOL (Extensible Authentication Protocol over LAN).
- The device side is another entity located at one end of the LAN segment, which authenticates the connected clients. The device side is usually a network device that supports the 802.1X protocol. It provides a port for the client to access the local area network. The port can be a physical port or a logical port.
- The authentication server is an entity that provides authentication services for the device. The authentication server is used to authenticate, authorize, and account for users, and is usually a RADIUS (Remote Authentication Dial-In User Service, Remote Authentication Dial-In User Service) server.

23.1.1.802.1X authentication method

The 802.1X authentication system uses EAP (Extensible Authentication Protocol, Extensible Authentication Protocol) to realize the exchange of authentication information between the client, the device and the authentication server.

- Between the client and the device, the EAP protocol packets are directly carried in the LAN environment using the EAPOL encapsulation format.
- There are two ways to exchange information between the device and the RADIUS server. One is that the EAP protocol packet is relayed by the device, and is carried in the RADIUS protocol using the EAPOR (EAP over RADIUS) encapsulation format; the other is that the EAP protocol packet is terminated by the device, using PAP (Password Authentication Protocol) , Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol, Challenge Handshake Authentication Protocol) attribute packets interact with the RADIUS server for authentication.

23.1.1.802.1X Basic Concepts

23.1.1.1. Controlled/Uncontrolled Ports

The device end provides a port for the client to access the LAN. This port is divided into two logical ports: a controlled port and an uncontrolled port. Any frame arriving at this port is visible on both the controlled port and the uncontrolled port.

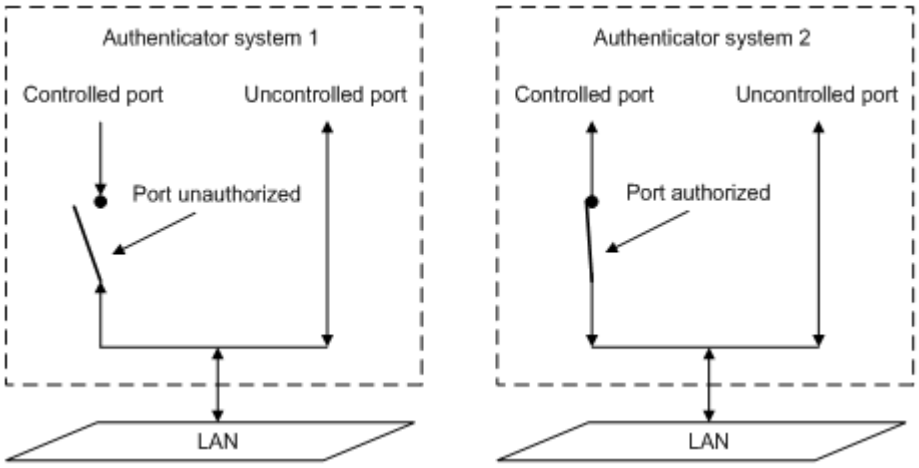
- The uncontrolled port is always in a two-way connection state and is mainly used to transmit EAPOL protocol frames to ensure that the client can always send or receive authentication packets.
- The controlled port is in a bidirectional connection state in the authorized state, and is used to transmit service packets; in the unauthorized state, it is forbidden to receive any packets from the client.

23.1.1.1. Authorized/Unauthorized Status

The device side uses the authentication server to authenticate the clients that need to access the local area network, and controls the authorized/unauthorized status of the controlled port according to the authentication result (Accept or Reject).

Figure 12 shows the effect of different authorization states on the controlled port on the packets passing through the port. The figure compares the port status of two 802.1X authentication systems. The controlled port of system 1 is in the unauthorized state (equivalent to the port switch being turned on), and the controlled port of system 2 is in the authorized state (equivalent to the port switch being turned off).

Figure 1-2 Effect of Authorization Status on Controlled Ports



The user can control the authorization status of the port through the access control mode configured under the port. The port supports the following three access control modes:

- Authorized-force mode: indicates that the port is always in the authorized state, allowing users to access network resources without authentication and authorization.
- Unauthorized-force mode: indicates that the port is always in an unauthorized state and does not allow users to authenticate. The device side does not provide authentication services for clients accessing through this port.
- Auto identification mode (auto): Indicates that the initial state of the port is an unauthorized state, which only allows EAPOL packets to be sent and received, and does not allow users to access network resources; if the authentication is passed, the port switches to the authorized state, allowing users to access network resources. This is also the most common situation.

23.1.1.1. Controlled Orientation

In the unauthorized state, the controlled port can be set as one-way controlled and two-way controlled.

- When the two-way control is implemented, the transmission and reception of frames are prohibited;
- When unidirectional control is implemented, it is forbidden to receive frames from the client, but it is allowed to send frames to the client.

23.1.1. **802.1X Authentication Process**

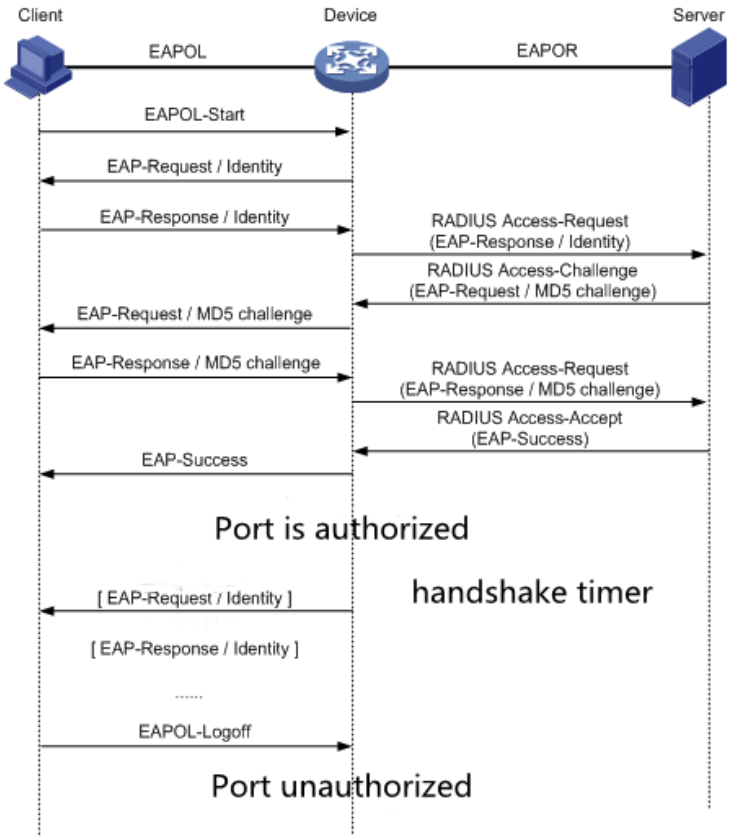
The 802.1X system supports EAP relay mode and EAP termination mode to interact with the remote RADIUS server to complete authentication. The following descriptions of the two authentication methods take the client's initiative to initiate authentication as an example.

23.1.1.1.EAP relay mode

This method is stipulated by the IEEE 802.1X standard, and EAP (Extensible Authentication Protocol) is carried in other high-level protocols, such as EAP over RADIUS, so that the extensible authentication protocol packets can reach the authentication server through complex networks. Generally speaking, the EAP relay mode requires the RADIUS server to support EAP attributes: EAP-Message and Message-Authenticator, which are used to encapsulate EAP packets and protect RADIUS packets that carry EAP-Message respectively.

The following takes the EAP-MD5 mode as an example to introduce the basic business process, as shown in Figure 1-3.

Figure 1-3 EAP relay business process of IEEE 802.1X authentication system



The certification process is as follows:

1) When the user needs to access the network, open the 802.1X client program, enter the user name and password that have been applied and registered, and initiate a connection request (EAPOL-Start message). At this point, the client program will send a message requesting authentication to the device to start an authentication process.

2) After receiving the data frame requesting authentication, the device will send a request frame (EAP-Request/Identity message) to request the user's client program to send the input user name.

3) The client program responds to the request sent by the device, and sends the user name information to the device through a data frame (EAP-Response/Identity message). The device sends the data frame sent by the client to the authentication server after packet processing (RADIUS Access-Request message).

4) After the RADIUS server receives the user name information forwarded by the device, it compares the information with the user name table in the database, finds the password information corresponding to the user name, and encrypts it with a randomly generated encrypted word. The encrypted word is sent to the device through a RADIUS Access-Challenge packet, and the device forwards it to the client program.

5) After the client program receives the encrypted word (EAP-Request/MD5 Challenge message) from the device, it uses the encrypted word to encrypt the password part (this encryption algorithm is usually irreversible) to generate EAP -Response/MD5 Challenge message, and send it to the authentication server through the device.

6) The RADIUS server compares the received encrypted password information (RADIUS Access-Request message) with the local encrypted password information. If they are the same, the user is considered to be a legitimate user, and the authentication passed message is returned (RADIUS Access-Accept message and EAP-Success message).

7) After receiving the authentication pass message, the device changes the port to the authorized state, allowing the user to access the network through the port. During this period, the device will monitor the user's online status by periodically sending handshake messages to the client. By default, if the two handshake request packets are not answered by the client, the device will log the user offline to prevent the device from being unable to sense that the user is offline due to abnormal reasons.

8) The client can also send an EAPOL-Logoff message to the device to actively request to go offline. The device side changes the port state from authorized state to unauthorized state, and sends an EAP-Failure message to the client.

23.2. CONFIGURE COMMAND

- Globally enable/disable 802.1X authentication

Command	SWITCH(config)# **dot1x enable** SWITCH(config)#**no dot1x enable**

Description	Globally enable and disable the 802.1X function.

- Port enable/disable 802.1X authentication

Command	SWITCH(config-if)# **dot1x port-control auto** SWITCH(config-if)#**no dot1x port-control auto**
Description	The port enables and disables the 802.1X function.

- Configure RADIUS server

Command	SWITCH(config)# **radius-server host** A.B.C.D **auth-port** <0-65535> **acct-port** <0-65535> **key** WORD SWITCH(config)#**no radius-server host** A.B.C.D
Description	Configure authentication server information. The default authentication port is 1812, and the accounting port is 1813. Make sure that the RADIUS server and device management addresses communicate with each other.

- Configure EAPOL protocol edition number

Command	SWITCH(config-if)# **dot1x protocol-version** <1-2> SWITCH(config-if)#**no dot1x protocol-version**
Description	Configure the version number of the EAPOL protocol on the specified port. Optional configuration, default is 2.

- Configure the authentication silent time

Command	SWITCH(config-if)# **dot1x quiet-period** <1-65535> SWITCH(config-if)#**no dot1x quiet-period**
Description	Configure the hold time of the HELD state. Optional configuration, the unit is seconds, the default is 60.

- Configure the re-authentication function

Command	SWITCH(config-if)# **dot1x reauthentication** SWITCH(config-if)#**no dot1x reauthentication**
Description	Configure the port to enable the re-authentication function. Optional configuration, disabled by default.

- Configure the maximum number of re-authentications

Command	SWITCH(config-if)# **dot1x reauthMax** <1-10> SWITCH(config-if)#**no dot1x reauthMax**

Description	Configure the maximum number of port re-authentications. If the number of re-authentication requests exceeds the limit and there is no response, the port becomes unauthorized. Optional configuration, default 2 times.

- Configure and enable the key transmission capability

Command	SWITCH(config-if)# **dot1x keytxenabled { disable | enable}**
Description	Configure the port key transfer function. Optional configuration, disabled by default.

- Configure the timer timeout time

Command	SWITCH(config-if)# **dot1x timeout {re-authperiod** <1-4294967295> **| server-timeout** <1-65535> **| supp-timeout** <1-65535> **| tx-period** <1-65535>**}** SWITCH(config-if)#**no dot1x timeout {re-authperiod | server-timeout | supp-timeout | tx-period}**
Description	Configure the port timer time. Optional configuration, the default re-authentication period is 3600 seconds, the server timeout is 30 seconds, the client authentication timeout is 30 seconds, and the client request timeout is 30 seconds.

- Globally enable/disable MAC authentication

Command	SWITCH(config)# **mac-auth enable** SWITCH(config)#**no mac-auth enable**
Description	Globally enable or disable the MAC authentication function.

- Port enable/disable MAC authentication

Command	SWITCH(config-if)# **mac-auth {enable | disable}**
Description	Enable or disable the MAC authentication function on the port.

- Port enable/disable MAC authentication dynamic VLAN delivery

Command	SWITCH(config-if)# **mac-auth dynamic-vlan-creation {enable | disable}**
Description	Enable or disable dynamic VLAN delivery of MAC authentication on the port. The current version does not support it.

- Configuring MAC authentication failure handling

Command	SWITCH(config-if)# **mac-auth auth-fail-action {drop-traffic | restrict-vlan** <2-4094>**}**
Description	Configure the behavior of MAC authentication failure. Optional configuration, default is drop-traffic: drop traffic. The current version does not support it.

- Configure the RADIUS server dead time

Command	SWITCH(config)# **radius-server deadtime** <0-1440> SWITCH(config)# **no radius-server deadtime**
Description	Configure the death time of the RADIUS server. During the authentication process, the dead server will be automatically skipped, and the non-dead server will be selected for authentication. Optional configuration, default is 0 minutes.

- Configure the default key of the RADIUS server

Command	SWITCH(config)# **radius-server key** STRING SWITCH(config)# **no radius-server key**
Description	Configure the default key of the RADIUS server. Optional.

- Configure the number of retransmissions by the RADIUS server

Command	SWITCH(config)# **radius-server retransmit** <1-100> SWITCH(config)# **no radius-server retransmit**
Description	Configure the number of retransmissions by the RADIUS server. Optional configuration, the default is 3 times.

- Configure the RADIUS server timeout period

Command	SWITCH(config)# **radius-server timeout** <1- 60> SWITCH(config)# **no radius-server timeout**
Description	Configure the RADIUS server timeout period. Optional configuration, default is 5 seconds.

23.3. CONFIGURE CASE

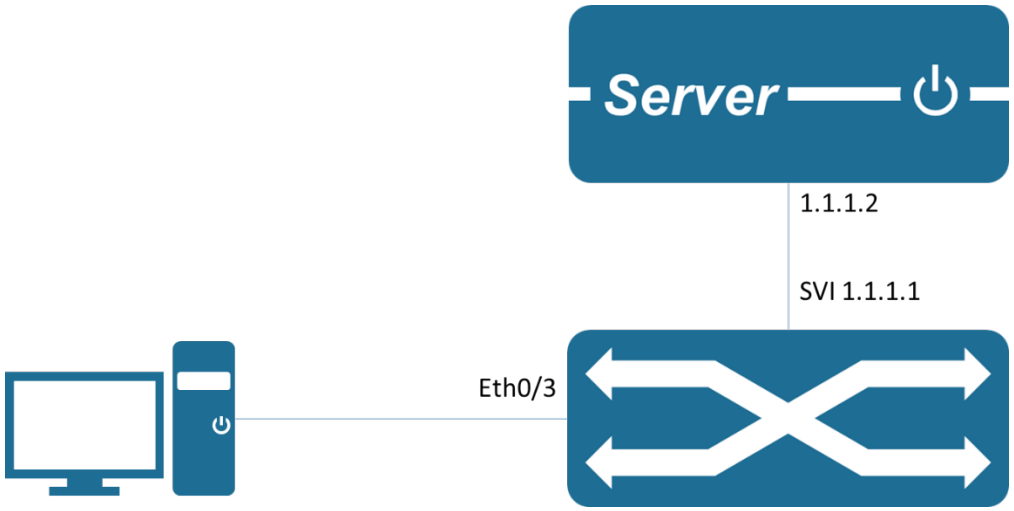
23.3.1.802.1X port authentication scenario

1) requirements

- It is required to authenticate access users on port GigabitEthernet0/3 to control their access to the Internet.
- RADIUS server group IP address 1.1.1.2.
- Set the shared key to name when the system exchanges packets with the RADIUS server.

2) Networking figure

Figure 1-4 802.1X authentication typical networking diagram



3) Typical configuration e.g.

Device ：

```
SWITCH(config)#dot1x enable
SWITCH(config)#interface gigabitEthernet0/3
SWITCH(config-if)#dot1x port-control auto
SWITCH(config-if)#exit
SWITCH(config)#radius-server host 1.1.1.2 key name
```

Server ：

Configure the NAS authentication device 1.1.1.1 and the communication key name.

Add user account test and password test.

Need to support the corresponding authentication method, such as EAP-MSCHAPv2

Client ：

Enable the 802.1X authentication client and log in with the account test.

The corresponding authentication method needs to be supported, such as the EAP-MSCHAPv2 method.

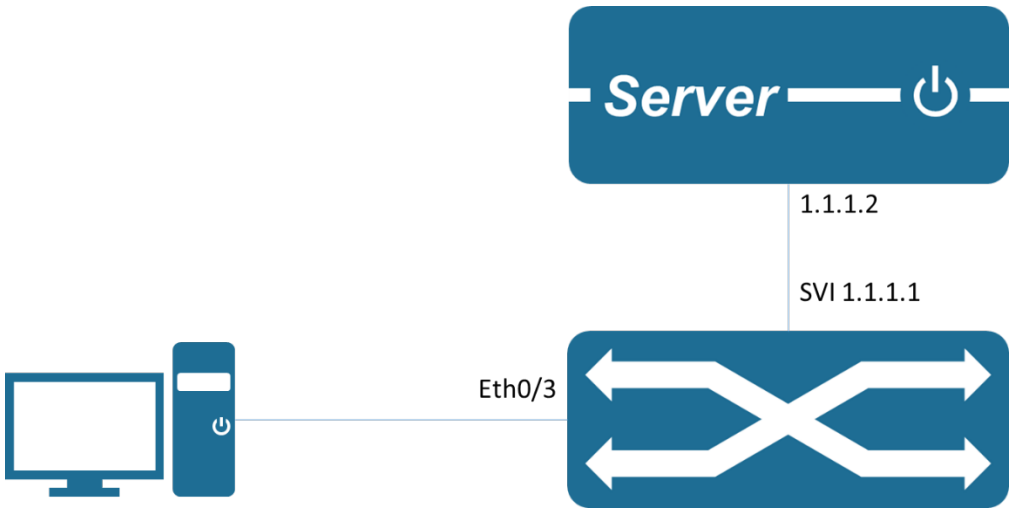
23.3.1. MAC Authentication Scenario

1) Requirements

- It is required to authenticate access users on port GigabitEthernet0/3 to control their access to the Internet.
- RADIUS server group IP address 1.1.1.2.
- Set the shared key to name when the system exchanges packets with the RADIUS server.

2) Networking Figure

Figure 1-5 Typical networking diagram of MAC authentication



3) Typical configuration e.g.

Device ：

```
SWITCH(config)# mac-auth enable
SWITCH(config)#interface gigabitEthernet0/3
SWITCH(config-if)#mac-auth enable
SWITCH(config-if)#exit
SWITCH(config)#radius-server host 1.1.1.2 key name
```

Server ：

Configure the NAS authentication device 1.1.1.1 and the communication key name.

Add the client MAC address as the user account and password to the user database.

Client ：

Enable the 802.1X authentication client and log in with any account.

23.4. DISPLAY COMMAND

- Display 802.1X port authentication information

```
SWITCH#show dot1x all
802.1X Port-Based Authentication Enabled
  RADIUS server address: 1.1.1.2:1812
  Next radius message id: 0
  RADIUS client address: not configured

802.1X info for interface gigabitEthernet0/6
  portEnabled: true - portControl: Auto
  portStatus: Unauthorized - currentId: 1
  protocol version: 2
  reAuthenticate: disabled
  reAuthPeriod: 3600
  abort:F fail:F start:F timeout:F success:F
  PAE: state: Connecting - portMode: Auto
  PAE: reAuthCount: 1 - rxRespId: 0
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle - reqCount: 0 - idFromServer: 0
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in - operControlledDirections: in
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
```

- Display MAC authentication information

```
SWITCH#show bridge
 Bridge    CVLAN  SVLAN  BVLAN  Port        MAC Address       FWD   Time-
out
 ---------+------+------+------+-----------+-----------------+-----+-----
----+
```

24. CONFIGURE PORT SECURITY

24.1. PORT SECURITY FUNCTION OVERVIEW

The Port Security function limits the number of valid MAC addresses on a port to restrict access to the port by illegal users. Packets with invalid MAC addresses are directly discarded.

Valid MACs can be generated statically or dynamically. Static valid MACs are generated through user command line configuration; dynamic valid MACs are dynamically generated through the MAC address learning function.

When the number of security addresses on the port has reached the maximum number of security addresses configured, the new MAC access port will be identified as an illegal MAC, and a violation event will be generated. The user can configure the response action when the violation event occurs, which is to restrict or shutdown the port respectively.

Restrict: prohibits illegal MAC data from passing through, and generates alarm log information. Illegal MAC will prohibit access to the port within the MAC address aging time. It can be restored through shutdown and no shutdown ports.

Shutdown: Force the port to go down, and configure the port recovery time. When the time is up, the port will automatically recover; it can also be recovered through the shutdown and no shutdown commands.

If you want to convert dynamic security users to static security users, you can enable the sticky function on the port. When the sticky function is enabled on the port, the dynamic users learned on the port will exist in the form of static users. If the configuration is saved, it will still exist after the device restarts.

Restriction Description

- Only support L2 port configuration port security, such as ordinary physical port, AP port.
- Only support the configuration of port security function in access mode.
- Do not support AP member port configuration port security function.
- Do not support SPAN destination port configuration port security function.
- Does not support the port security function on ports that have been configured with static MAC addresses.

24.2. CONFIGURE COMMAND

- Enable the port security function

Command	SWITCH(config-if)#**switchport port-security** SWITCH(config-if)#**no switchport port-security**
Description	Enable/disable the port security function on the interface

- Configure the maximum number of secure addresses on a port

Command	SWITCH(config-if)#**switchport port-security maximum** VALUE SWITCH(config-if)#**no switchport port-security maximum**
Description	The default maximum number of secure addresses is 1 Range<1 1024>

- Configure a static security address

Command	SWITCH(config-if)#**switchport port-security mac-address** MAC_ADDR SWITCH(config-if)#**no switchport port-security mac-address** MAC_ADDR
Description	Secure address format: XXXX.XXXX.XXXX The secure address cannot be a broadcast or multicast address

- Configure the port security sticky function

Command	SWITCH(config-if)# **switchport port-security mac-address sticky** SWITCH(config-if)#**no switchport port-security mac-address sticky**
Description	Turn on/off sticky function

- Configure the security address aging time

Command	SWITCH(config-if)#**switchport port-security aging time** MINUTES SWITCH(config-if)#**no switchport port-security aging time**
Description	The default aging time is 0, which means that the aging function is disabled. Aging Time Range <0 1440> The default aging function only takes effect for dynamic and sticky security addresses

- Configure and enable the static security address aging function

Command	SWITCH(config-if)# **switchport port-security aging static** SWITCH(config-if)#**no switchport port-security aging static**
Description	Enable aging static security addresses

- Configuring port security violation handling

Command	SWITCH(config-if)# **switchport port-security violation** { **strict** | **shutdown** } SWITCH(config-if)#**no switchport port-security violation**
Description	Default exception handling mode restrict Restrict: prohibit illegal user data from passing, and log prompt Shutdown: Shutdown the port and restore after errdisable recovery time Through the shutdown/no shutdown command, it can also be restored

24.3. DISPLAY COMMAND

In privileged mode, you can view port security configuration information, security address information, etc.

- Display all port security summary information

```
SWITCH#show port-security brief
interface    mac-address      mac-address      violation      violation
               maxinum            count            count      action
-------------------------------------------------------------------------------------------
GiE0/1       10                 3                0              shutdown
GiE0/2       1                  0                0              restrict
GiE0/3       1                  0                0              restrict
GiE0/4       1                  0                0              restrict
GiE0/5       1                  0                0              restrict
GiE0/6       1                  0                0              restrict
GiE0/7       1                  0                0              restrict
GiE0/8       1                  0                0              restrict
```

- Display interface port security information

```
SWITCH#show port-security interface gigabitEthernet0/1
Port Security                 : Enabled
Maimum MAC Addresses          : 10
Violation Mode                : Shutdown
Aging Time(mins)              : 10
Aging static                  : Enabled
Total MAC Addresses           : 3
Configured MAC Addresses      : 2
Security Violation Count      : 0
Last Violate Address          : --
```

- Display security address information

```
SWITCH#show port-security mac-address
interface    vlan      mac-address           type          left-time(min)
-------------------------------------------------------------------------------
GiE0/1       1         0001.0002.0004        static        10
```

```
GiE0/1          1          0001.0002.0003          static          10
GiE0/1          1          000e.c6c1.3a03          dynamic         10
```

- Display interface security address information

```
SWITCH#show port-security mac-address interface gigabitEthernet0/1
interface      vlan       mac-address              type             left-time(min)
-------------------------------------------------------------------------------
GiE0/1          1          0001.0002.0004          static          10
GiE0/1          1          0001.0002.0003          static          10
GiE0/1          1          000e.c6c1.3a03          dynamic         10
```

24.4. TYPICAL CASE

- The number of legal users on interface gigabitEthernet0/1 is limited to 3, and illegal users cannot access the device

```
SWITCH(config-if)#switchport port-security
SWITCH(config-if)#switchport port-security maximum 3
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0001
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0002
SWITCH(config-if)#switchport port-security mac-address 0001.0001.0003
```

25. CONFIGURE IP SOURCE GUARD

25.1. IP SOURCE GUARD FUNCTION OVERVIEW

The Ip Source Guard binding function allows IP packets that conform to the IP+MAC binding to pass through the port, and those that do not conform are directly discarded, thereby preventing IP/MAC spoofing attacks.

The binding entries of Ip Source Guard mainly come from two sources: user static configuration and dynamic acquisition in the ip dhcp snooping environment.

User static configuration: It mainly deals with host users whose IP addresses are statically configured in the local area network.

Ip dhcp snooping dynamic acquisition: It mainly deals with host users who dynamically acquire IP addresses through dhcp in the local area network.

IP/MAC spoofing attack: An illegal MAC user sends an IP packet with a legitimate source IP to legalize the access identity.

Restriction Description

- The current software version only supports the static configuration mode of the binding entry user.
- Does not support the configuration of Ip Source Guard on AP member ports.

25.2. CONFIGURE COMMAND

- Enable Ip Source Guard function

Command	SWITCH(config-if)#**ip verify source** SWITCH(config-if)#**no ip verify source**
Description	Enable/disable the Ip Source Guard function on the interface

- Configuring binding entries

Command	SWITCH(config)# **ip source binding** XXXX.XXXX.XXXX **vlan** VALUE A.B.C.D **interface** IFNAME SWITCH(config)#**no ip source binding** XXXX.XXXX.XXXX **vlan** VALUE A.B.C.D **interface** IFNAME
Description	Secure address format: XXXX.XXXX.XXXX IP address format: A.B.C.D A single port can be configured with a maximum of 128 entries

25.3. DISPLAY COMMAND

In privileged mode, you can view the binding items of the ip verify source effective rule and ip source binding.

- Check the effective rules of ip verify source

```
SWITCH#show ip verify source
interface   Filter-type   Filter        IP-address        Mac-address    vlan
------------------------------------------------------------------------
GiE0/1        Ip            Permit      1.1.1.1           0001.0001.0001 1
GiE0/1        Ip            Deny        All               All            All
GiE0/2        Ip            Deny        All               All            All
```

- Check the effective rules of port ip verify source

```
SWITCH#show ip verify source interface gigabitEthernet0/1
interface   Filter-type   Filter        IP-address        Mac-address    vlan
-----------------------------------------------------------------------------------------
GiE0/1        Ip            Permit      1.1.1.1           0001.0001.0001 1
GiE0/1        Ip            Deny        All               All            All
```

- Display ip source binding entry

```
SWITCH#show ip source binding
interface   vlan   IP-address        Mac-address      Lease      Type
-----------------------------------------------------------------------------------------
GiE0/1        1       1.1.1.1           0001.0001.0001 infinite      static
GiE0/2        1       1.1.2.1           0001.0002.0001 infinite      static
```

- Display interface ip source binding entry

```
SWITCH#show ip source binding
interface   vlan   IP-address        Mac-address      Lease      Type
-----------------------------------------------------------------------------------------
GiE0/1        1       1.1.1.1           0001.0001.0001 infinite      static
```

25.4. TYPICAL CASE

- The DHCP server has three users connected to the gigabitEthernet0/1 port, which is required to prevent IP/MAC attacks of illegal users in the LAN

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#ip verify source
SWITCH(config)#ip source binding 0001.0001.0001 vlan 1 1.1.1.10 interface
gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0002 vlan 1 1.1.1.11 interface
gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0003 vlan 1 1.1.1.12 interface
gigabitEthernet0/1
```

26. CONFIGURE ARP-CHECK

26.1. ARP-CHECK FUNCTION OVERVIEW

Arp-check (ARP packet inspection) function, filters all ARP packets under the port and discards all illegal ARP packets, which can effectively prevent ARP spoofing in the network and improve the stability of the network.

In devices that support the Arp-check function, the Arp-check function can generate corresponding ARP filtering information according to the legitimate user information (IP+MAC) generated by security application modules such as IP Source Guard, so as to realize the detection of illegal ARP reports in the network. text filtering.

Restriction Description

- Arp-check function is not supported on AP member ports.

26.2. CONFIGURE COMMAND

- Enable Arp-check function

Command	SWITCH(config-if)#**arp-check** SWITCH(config-if)#**no arp-check**
Description	Enable/disable the Arp-check function on the interface

26.3. TYPICAL CASE

- The DHCP server has three users connected to the gigabitEthernet0/1 port. It is required to prevent illegal user IP/MAC attacks in the LAN and enable illegal ARP attack detection.

```
SWITCH(config)#interface gigabitEthernet0/1
SWITCH(config-if)#ip verify source
SWITCH(config-if)#arp-check
SWITCH(config)#ip source binding 0001.0001.0001 vlan 1 1.1.1.10 interface
gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0002 vlan 1 1.1.1.11 interface
gigabitEthernet0/1
SWITCH(config)#ip source binding 0001.0001.0003 vlan 1 1.1.1.12 interface
gigabitEthernet0/1
```

27. CONFIGURE SNMP NETWORK MANAGEMENT

27.1. OVERVIEW

SNMP is the abbreviation of Simple Network Management Protocol, which became a network management standard RFC1157 in August 1988. Up to now, due to the support of this protocol by many manufacturers, SNMP has become the de facto network management standard and is suitable for use in the interconnected environment of multi-manufacturer systems.

Using the SNMP protocol, network administrators can perform information query, network configuration, fault location, and capacity planning for nodes on the network. Network monitoring and management are the basic functions of SNMP.

Currently the following versions of SNMP exist:

SNMPv1: The first official version of the Simple Network Management Protocol, defined in RFC1157.

SNMPv2C: Community-Based SNMPv2 Management Architecture, defined in RFC1901.

SNMPv3: By authenticating and encrypting data, it provides the following security features:

1) Ensure that the data is not tampered with during transmission.
2) Make sure that the data is sent from a legitimate data source.
3) Encrypt the message to ensure the confidentiality of the data.

27.2. CONFIGURE COMMAND

- Configure the communication community word

Command	SWITCH(config)#**snmp-server community** COMMUNITY **{ro | }** SWITCH(config)#**no snmp-server community** COMMUNITY
Description	Configure/delete SNMP communication community word; ro: read-only identifier, configure the community word as a community word with only read permission; the default configuration is a community word with both read and write permissions; Supports configuring multiple community characters at the same time

- Configure SNMPv3 view

Command	SWITCH(config)# **snmp-server view** NAME **{include | exclude}** OID SWITCH(config)# **no snmp-server view** NAME

Description	Configure/delete SNMPv3 views; Supports configuring multiple views at the same time, and supports configuring multiple rules for a single view; The system has all and none views by default and cannot be modified

- Configure SNMP group

Command	SWITCH(config)# **snmp-server group** NAME **{v3 | } {noAuthNoPriv | authNoPriv | authPriv} read** RVIEW **write** WVIEW SWITCH(config)# **snmp-server group** NAME **{v1 | v2c} read** RVIEW **write** WVIEW SWITCH(config)# **no snmp-server group** NAME
Description	configure/delete SNMP groups; Support to configure multiple groups at the same time; SNMPv1 and SNMPv2c will automatically create group information in order to be compatible with the old configuration when configuring the community, usually without additional attention

- Configure SNMPv3 users

Command	SWITCH(config)# **snmp-server user** NAME **group** GROUPNAME **auth {md5 | sha}** {AUTHPASS} **priv {aes | des}** PRIVPASS SWITCH(config)# **no snmp-server user** NAME
Description	configure/delete SNMP users; Support to configure multiple users at the same time;

- Configure SNMP Host notification server

Command	SWITCH(config)# **snmp-server host** IPADDR **{informs | traps} {v3 |} {noAuthNoPriv | authNoPriv | authPriv} user** NAME SWITCH(config)# **snmp-server host** IPADDR **{informs | traps} {v1 | v2c} community** NAME SWITCH(config)# **no snmp-server host** NAME
Description	configure/delete SNMP server;

	Support to configure multiple servers at the same time;

27.3. CONFIGURE CASE

Case requirements: The IP address of the SNMP network management server is 2.2.2.2, and the read-write communication group word is unified as public.

- Enter the global configuration mode to configure:

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#snmp-server community public
SWITCH(config)#snmp-server 2.2.2.2 community public
SWITCH(config)#
```

Case requirements: The IP address of the SNMP network management server is 2.2.2.2, SNMPv3 is used, the user test password is 12345678, the encryption key is 87654321; the authentication algorithm MD5, the encryption algorithm DES

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)# snmp-server group test v3 authPriv read all write all
SWITCH(config)# snmp-server user test group test auth MD5 12345678 priv
DES 87654321
SWITCH(config)# snmp-server host 2.2.2.2 informs v3 authPriv user test
```

28. CONFIGURE RMON

28.1. OVERVIEW

SNMP is the most widely used network management protocol in the Internet. The collection and statistics of network communication information are realized through the agent software embedded in the device. The management software obtains the information by sending query signals to the MIB of the agent through polling, and realizes the management of the network through the obtained information. Although the MIB counter records the sum of the statistics, it does not allow historical analysis of the day-to-day communication situation. In order to comprehensively check the traffic and traffic changes in a day, the network management software needs to continuously poll to analyze the network status through the obtained information.

Polling with SNMP has two distinct disadvantages:

- Occupies a lot of network resources. In a large-scale network, a large number of network communication packets will be generated by polling, which will cause network congestion and even cause network congestion. Therefore, SNMP is not suitable for managing large-scale network traffic. The network is not suitable for recycling large amounts of data, such as routing table information.
- Increases the burden of the administrator. The task of collecting data in SNMP polling is done by the network administrator through the network management software. If the network administrator monitors more than 3 network segments, it may occur due to excessive burden. A situation in which the network administrator cannot complete the task.

In order to improve the availability of management information, reduce the burden of management stations, and meet the needs of network administrators to monitor the performance of multiple network segments, IETF developed RMON to solve the limitations of SNMP in the expanding distributed interconnection. The monitoring function of the data traffic of the network segment and even the entire network. The following are the features of RMON:

- SNMP is the basis for the realization of RMON, and RMON is the enhancement of SNMP functions

RMON is implemented based on the SNMP architecture and is compatible with the existing SNMP framework. It is still composed of the network management workstation NMS and the agent agent running on each network device. Because RMON does not use another set of mechanisms, the network management workstation NMS and SNMP are shared, and the network management personnel do not need to carry out additional learning, so the implementation is relatively simple.

- RMON enables SNMP to monitor remote network devices more effectively and proactively, and provides an efficient means for monitoring the operation of the network.

The RMON protocol stipulates that the managed device can automatically send Trap information when the alarm threshold is reached, so the management device does not need to obtain the value of the MIB variable through polling multiple times for comparison. The purpose of efficiently managing large interconnected networks.

RMON allows multiple monitors, and monitors can collect data in the following two ways:

- Through a dedicated RMON Probe (detector), the NMS directly obtains management information from the RMON Probe and controls network resources. In this way, all information of the RMON MIB can be obtained.
- Embed RMON Agent directly into network devices, making them network devices with RMON Probe function. The NMS uses SNMP to exchange data information with it and collect network management information. This method is limited by device resources and generally cannot obtain all the data of the RMON MIB. Basically, only four groups (alarms, events, history, and statistics) are collected.

Our equipment adopts the second method and implements the RMON Agent function on the equipment. Through this function, the management device can obtain information such as overall traffic, error statistics, and performance statistics on the network segment connected to the managed network device interface, thereby realizing network monitoring.

28.2. PRINCIPLE

Before configuring RMON, you need to understand the basic concepts of the four groups of statistics, history, alarms, and events defined by the RMON specification.

RMON feature

RMON mainly implements statistics and alarm functions, and is used for remote monitoring and management of managed devices by management devices in the network.

The RMON statistics function can be implemented through the RMON statistics group or the RMON history group, which are divided into Ethernet statistics functions and historical statistics functions.

- Ethernet statistics function (corresponding to the statistics group in the RMON MIB): The system collects basic statistics of each network being monitored. The system will continuously count the traffic of a certain network segment and the distribution of various types of packets, or the number of error frames of various types, the number of collisions, etc. The statistical objects include the number of network collisions, the number of CRC check error packets, the or oversized), the number of broadcast and multicast packets, the number of bytes received, the number of received packets, etc.

- Historical statistics function (corresponding to the history group in the RMON MIB): The system periodically samples and collects network status statistics and stores them for subsequent processing. The system will periodically collect statistics on various traffic information, including bandwidth utilization, number of error packets and total number of packets.

The RMON alarm function includes the event definition function and the alarm threshold setting function. The RMON alarm function is realized by the combination of these two sub-functions.

- Event definition function (corresponding to the event group in the RMON MIB): The event group controls the events and prompts from the device, and provides all the events generated by the RMON Agent. When an event occurs, it can record logs or send Trap to the network management station.
- Set alarm threshold function (corresponding to the alarm group in the RMON MIB): The system monitors the specified alarm variable (the OID corresponding to any alarm object). After the user pre-defines a set of thresholds and sampling time for the specified alarm, the system will obtain the value of the specified alarm variable according to the defined time period. When the value of the alarm variable is greater than or equal to the upper threshold, an upper alarm event will be triggered; When the value of the variable is less than or equal to the lower limit threshold, a lower limit alarm event is triggered. RMON Agent will record the above monitored status as a log or send Trap to the network management station.

Multiple RMON groups are defined in the RMON specification (RFC2819), and the device implements four groups of statistics, history, alarm, and events supported in the public MIB. These groups are introduced separately below.

- **Statistics group**

The statistics group specifies that the system will continuously collect statistics on various traffic information of the Ethernet interface, and store the statistical results in the Ethernet statistics table (etherStatsTable) for the management device to view at any time. Statistics include the number of network collisions, the number of CRC check error packets, the number of data packets that are too small (or too large), the number of broadcast and multicast packets, the number of bytes received, and the number of received packets.

After the statistics entry is successfully created on the specified interface, the statistics group collects statistics on the number of packets on the current interface, and the statistics result is a continuous accumulated value.

- **History group**

The history group periodically collects network status statistics and stores them for subsequent processing.

The history group contains two tables:

- History ControlTable (historyControlTable): mainly used to set the sampling interval and other control information.
- Ether History Table (etherHistoryTable): It is mainly used to store the historical data collected by the historical group periodically to collect network status statistics, and to provide network administrators with historical data on network segment traffic, error packets, broadcast packets, utilization, and collision times and other statistical information.

- **Event groups**

The event defined by the event group is used in the alarm group configuration item and the extended alarm group configuration item. When the monitoring object reaches the alarm condition, the event will be triggered. RMON event management is to add events to the specified row of the event table and define how the events are handled:

- log: Only logs are sent
- trap: only send trap messages to NMS
- log-trap: Send both logs and trap messages to NMS
- none: do nothing

- **Alarm group**

Alarm groups allow monitoring of a predefined set of thresholds for alarm variables (which can be arbitrary objects in the local MIB). After the user defines the alarm table item (alarmTable), the system will obtain the value of the monitored alarm variable according to the defined time period. When the value of the alarm variable is greater than or equal to the upper limit threshold, an upper limit alarm event will be triggered; If the value is less than or equal to the lower limit threshold, a lower limit alarm event is triggered, and the alarm management will perform corresponding processing according to the definition of the event.

28.3. CONFIGURE COMMAND

- Configure the statistics group

Command	SWITCH(config)# **rmon statistics** <1-65535> **interface** IFNAME **{owner** OWNERNAME **|}** SWITCH(config-if)#**no rmon statistics** <1-65535>

Description	configure/delete statistics group; <1-65535>: Group index IFNAME: interface name OWNERNAME: owner information

- Configure history group

Command	SWITCH(config)# **rmon history** <1-65535> **interface** IFNAME **buckets** <1-65535> **interval** <1-3600> **{owner** OWNERNAME **|}** SWITCH(config-if)#**no rmon history** <1-65535>
Description	configure/delete history group; <1-65535>: Group index IFNAME: interface name <1-65535>: History bucket size <1-3600>: Recording period; the unit is seconds OWNERNAME: owner information

- Configure event groups

Command	SWITCH(config)# **rmon event** <1-65535> **{description** DESCRIPTION **|} {log | trap** COMMUNITY **| log-trap** COMMUNITY **| none} {owner** OWNERNAME **|}** SWITCH(config-if)#**no rmon event** <1-65535>
Description	configure/delete event groups; <1-65535>: Group index DESCRIPTION: Event description COMMUNITY: Trap communication group word OWNERNAME: owner information

- Configure alarm groups

Command	SWITCH(config)# **rmon alarm** <1-65535> **object** STRING <1-65535> **{absolute | delta} rising-threshold** <1-2147483645> <1-65535> **falling-threshold** <1-2147483645> <1-65535> **{owner** OWNERNAME **|}** SWITCH(config-if)#**no rmon alarm** <1-65535>
Description	Configure/delete alarm groups; <1-65535>: Group index STRING: OID of alarm monitoring; for example, 1.3.6.1.2.1.2.2.1.10.1 indicates the number of bytes received by monitoring interface 1 <1-65535>: Monitoring period; the unit is seconds <1-2147483645>: Rising Threshold <1-65535>: Rising event index; corresponds to the index in the event group <1-2147483645>: Falling Threshold <1-65535>: Fall event index; corresponds to the index in the event group OWNERNAME: owner information

- Configure the upper limit of log entries

Command	SWITCH(config)# **rmon max-log** <1-65535> SWITCH(config-if)#**no rmon max-log**
Description	Configure/reset the upper limit of log entries; <1-65535>: Number of entries The log here refers to the log generated by the event group, not the system log The default upper limit is 100; when the number of logs generated exceeds the limit of entries, the old logs will be deleted according to the generation time to maintain the upper limit

28.4. CONFIGURE CASE

Requirements

The IP address of the SNMP network management server is 2.2.2.2, and the community word for read and write communication is public.

The network management server needs to query the traffic of port 1 of the device through rmon

The network management server needs to monitor the input traffic of port 1 of the device through rmon. The cycle is 10 seconds. Once the number of input bytes changes by more than 1MB (1000000B), an alarm is triggered and a log is recorded.

Configure steps:

Initialize the network management configuration

```
SWITCH#
SWITCH#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SWITCH(config)#snmp-server community public
SWITCH(config)#snmp-server 2.2.2.2 community public
SWITCH(config)#
```

Configure the rmon statistics group (the following rmon configurations can be configured on the NMS through the MIB)

SWITCH(config)# rmon statistics 1 interface gigabitEthernet0/1 owner abc

Configure rmon events and alarm groups (the following rmon configurations can be configured on the NMS through MIB)

```
SWITCH(config)# rmon event 1 log-trap public owner abc
SWITCH(config)# rmon alarm 1 object 1.3.6.1.2.1.2.2.1.10.1 10 delta
rising-threshold 1000000 1 falling-threshold 1000000 1
```

28.5. DISPLAY COMMAND

- Display event group log

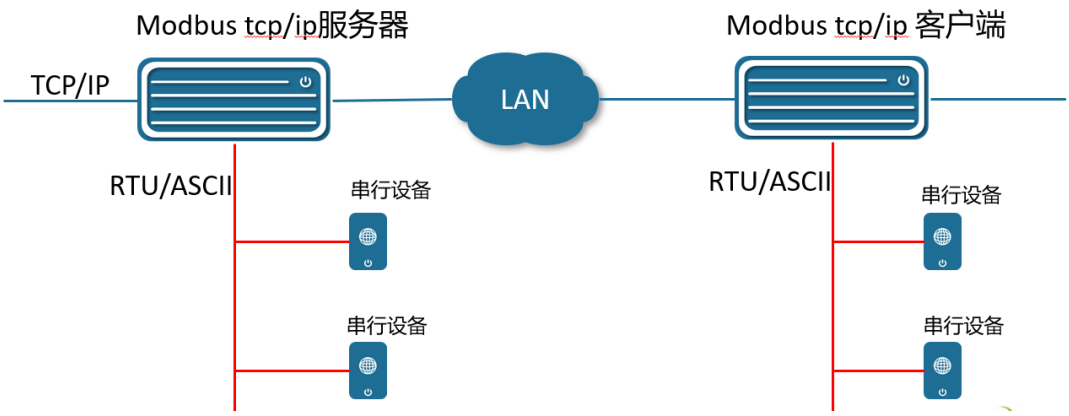
```
SWITCH#show rmon log
event 1 log 226 time 2304 desc
event 1 log 227 time 2314 desc
event 1 log 228 time 2324 desc
event 1 log 229 time 2334 desc
event 1 log 230 time 2344 desc
event 1 log 231 time 2354 desc
event 1 log 232 time 2364 desc
event 1 log 233 time 2374 desc
……
```

29. CONFIGURE MODBUS

29.1. OVERVIEW

Modbus is a serial communication protocol that was published by Modicon in 1979 for communication using programmable logic controllers (PLCs). At present, it has become an industry standard for communication protocols in the industrial field, and is a common connection method between industrial electronic devices.

Modbus is an application layer transmission protocol on the seventh layer of the OSI model. It provides a client-server communication model between devices connected to different types of buses or networks. The typical modbus communication structure is shown in the following figure:



TCP/IP Ethernet part: based on IETF standards: RFC793, RFC791,

Modbus tcp/ip client: As a client, the device actively connects to the server device on the Ethernet. Need to tell the client device, server network address and TCP port number through settings. After the connection is established, the client device transmits the data received from RTU/ASCII to the server through the TCP/IP network, and vice versa, the data received from the server will be transmitted to the corresponding serial device through RTU/ASCII.

Modbus tcp/ip server: As a server, it is passively connected. One of the most critical parameters is the [local port], which supports the connection of multiple clients.

RTU/ASCII part: Based on TIA, EIA standards: 232-E, 485A, it defines the packet packaging and decoding methods for data transmission on serial links. According to the definition in GB-T19582, RTU mode is required, and ASCII mode is optional.

29.2. DISPLAY COMMAND

- Configure modbus-tcp working mode

Command	SWITCH(config)# **modbus-tcp mode {client | server }**
Description	Client mode: The tcp side is in client mode, and the packets are forwarded between ip-rtu, without paying attention to the content Server mode: The tcp side is in server mode, and the packets are forwarded between ip-rtu, without paying attention to the content Default is client mode When the mode is switched, other configurations in the original mode are retained Currently only supports client mode

- Configure modbus-tcp server

Command	SWITCH(config)# **modbus-tcp server ip** IPADDR **port** L4-PORT SWITCH(config-if)**#no modbus-tcp server**
Description	This command is supported in client mode, and returns configuration failure in server mode Port range <1 65535>

- Configure modbus-tcp local

Command	SWITCH(config)# **modbus-tcp local port** L4-PORT
Description	This command is supported in server mode, and configuration failure is returned in client mode Port range <1 65535> Not supported currently

- Configure the heartbeat keyword

Command	SWITCH(config)# **modbus-tcp server keep-alive keywords** KEYWORD SWITCH(config)#**no modbus-tcp server keep-alive keywords**
Descriptin	This command is supported in client mode, and returns configuration failure in server mode Keyword length does not exceed 32 bytes

- Configure the heartbeat interval

Command	SWITCH(config)# **modbus-tcp server keep-alive interval** SECOND SWITCH(config)#**no modbus-tcp server keep-alive interval**
Description	This command is supported in client mode, and returns configuration failure in server mode Time interval range <1 86400> seconds The default time interval is 60 seconds

- Configure serial port parameters

Command	SWITCH(config)# **modbus-rtu** ID **baud-rate (9600 | 19200 | 38400 | 57600 | 115200) data-bits (7 | 8) parity (even | odd | none) stop-bits (1 | 2)** SWITCH(config-if)#**no modbus-rtu <1-4>**
Description	The ID range is <1-4>, and the legal ID can be found through the show modbus summary command. Default baud-rate 115200, data-bits 8 bits, parity none, stop-bits 1 bit

29.3. CONFIGURE CASE

Requirements

The device is modbus-tcp client, connected to server 192.168.64.1, server port 1024

Heartbeat keyword "hello", heartbeat interval default

Device RTU-1 downlink IO device, baud-rate 115200, parity "even", data-bits 8, stop-bits 1

Configure steps

```
        SWITCH#
        SWITCH#configure terminal
        Enter configuration commands, one per line.  End with CNTL/Z.
        SWITCH(config)#modbus-tcp server ip 192.168.64.1 port 1024
        SWITCH(config)# modbus-tcp server keep-alive keywords hello
        SWITCH(config)# modbus-rtu 1 baud-rate 115200 data-bits 8 parity even
stop-bits 1
```

29.4. DISPLAY COMMAND

- Display modbus configuration information

```
SWITCH#show modbus summary
Modbus-tcp server
    host        : 192.168.64.1
    port        : 1024
    keywords    : hello
    interval    : 60 seconds

Modbus-rtu 1
    baud-rate   : 115200
    data-bits   : 8
    parity      : even
    stop-bits   : 1
```

- Display modbus-tcp connect state information

```
SWITCH#show modbus status
Tcp-mode    Status  Remote                  Local                   Keep-alive
-------------------------------------------------------------------------------
tcp-client  link    192.168.64.1:1024       192.168.64.100:47188    0
```

- Display statistics

```
SWITCH#show modbus statistic
    Tcp Octets Rx                 :   5824
    Tcp Packets Rx                :   728
    Tcp Err Packets Rx            :   53
    Tcp Last Packet Rx Err Reason :   badcrc
    Tcp Connect Up/Down times     :   1
    Tcp Overload Drop Packets     :   29
    Tcp Err Packets Tx            :   0
    Rtu Err Packets               :   6
    Rtu Last Packet Err Reason    :   timeout
```

30. CONFIGURE IO

30.1. CONFIGURE COMMAND

- Configure IO output level

Command	SWITCH(config)# **io-ctrl** ID **level (high | low)**
Description	The ID can be viewed from the show io-ctrl summary command High: High level Low: low level This command is only supported by the IO of the output attribute

30.2. DISPLAY COMMAND

- Display IO information

```
SWITCH#show io-ctrl summary
ioid  direction   level   capacity    direction
------------------------------------------------------------
1     output      high    output
2     input       high    input
```

31. CONFIGURE DHCP SERVER

31.1. PROTOCOL OVERVIEW

DHCP (Dynamic Host Configuration Protocol) is a local area network network protocol that works using the UDP protocol and is widely used to dynamically allocate reusable network resources such as IP addresses.

DHCP is based on the Client/Server working mode. The DHCP client obtains the IP address and other configuration information from the DHCP server by sending a request message. When the DHCP client and server are not on the same subnet, there must be a DHCP relay agent (DHCP Relay) to forward DHCP request and reply messages.

31.1.1. Protocol Standards

RFC2132 DHCP Options and BOOTP Vendor Extensions. S. Alexander, R. Droms. March 1997. (Format: TXT, HTML) (Obsoletes RFC1533) (Updated by RFC3442, RFC3942, RFC4361, RFC4833, RFC5494) (Status: DRAFT STANDARD) (DOI: 10.17487/RFC2132)

31.2. CONFIGURE COMMAND

31.2.1. **Global mode configure command**

- Globally enable/disable DHCP server

Command	SWITCH(config)# **ip dhcp-server enable** SWITCH(config)#**no ip dhcp-server enable**
Description	Globally enable and disable the DHCP server.

- Configure global parameters

Command	SWITCH(config)# **ip dhcp-server parameter** NAME VALUE SWITCH(config)# **ip dhcp-server parameter (authoritative (on|off) | server-name** NAME **| server-identifier** IDENTIFY **| default-lease-time** <1-2147483648> **| max-lease-time** <1-2147483648> **| ping-timeout-ms** <1-65535> **| ping-timeout** <1-65535>**)** SWITCH(config)# **no ip dhcp-server parameter** NAME

	SWITCH(config)# **no ip dhcp-server parameter (authoritative | server-name | server-identifier | default-lease-time | max-lease-time | ping-timeout-ms | ping-timeout)**
Description	Global parameter configuration. When parameter values conflict, global parameters take precedence over parameters for subnets and address pools with more precise ranges. Default lease time: 43200s/12h Optional.

- Configure global options

Command	SWITCH(config)# **ip dhcp-server option** NAME VALUE SWITCH(config)# **ip dhcp-server option (routers** A.B.C.D **| domain-name** NAME **| domain-name-servers** A.B.C.D **| capwap-ac-v4** A.B.C.D**)** SWITCH(config)# **no ip dhcp-server option** NAME SWITCH(config)# **no ip dhcp-server option (routers | domain-name | domain-name-servers | capwap-ac-v4)**
Description	Global option configuration. When option values conflict, global options take precedence over options for subnets and address pools with more precise ranges. Optional.

- Configure custom domain fields

Command	SWITCH(config)# **ip dhcp-server custom-space** NAME **[code width** <1-4>**] [length width** <1-4>**] [hash size** <1-65535>**]** SWITCH(config)#**no ip dhcp-server custom-space** NAME
Description	Configure custom domain information fields. Optional.

- Configure custom options

Command	SWITCH(config)# **ip dhcp-server custom-option** NAME **code** <1-255> **(boolean|integer|ip-address|text|string|encapsulate)** SWITCH(config)#**no ip dhcp-server custom-option** NAME
Description	Configure custom options fields. The configured custom option code value must not conflict with the configured normal options. Optional.

- Configure forced send options

Command	SWITCH(config)# **ip dhcp-server force-option** <1-255> SWITCH(config)#**no ip dhcp-server force-option** <1-255>
Description	Configure mandatory options fields. Optional.

- Configure static address

Command	SWITCH(config)# **ip dhcp-server static-lease** NAME XX:XX:XX:XX:XX:XX A.B.C.D SWITCH(config)#**no ip dhcp-server static-lease** NAME
Description	Configure static address binding. Optional.

- Configure the whitelist

Command	SWITCH(config)# **ip dhcp-server whitelist** NAME XX:XX:XX:XX:XX:XX SWITCH(config)#**no ip dhcp-server whitelist** NAME
Description	Configure a whitelist. Optional.

- Configure the blacklist

Command	SWITCH(config)# **ip dhcp-server blacklist** NAME XX:XX:XX:XX:XX:XX SWITCH(config)#**no ip dhcp-server blacklist** NAME
Description	Configure the blacklist. Optional.

- Configure custom classification

Command	SWITCH(config)# **ip dhcp-server class** NAME **match** EXP SWITCH(config)#**no ip dhcp-server class** NAME
Description	Configure custom taxonomies. For professional usage, please configure it under the guidance of technicians. E.g.： ip dhcp-server class win_pc match "substring (option vendor-class-identifier,0,4)=MSFT" OPTIONAL .

31.2.2. Subnet Configuration Commands

- Configure subnet information

Command	SWITCH(config)# **ip dhcp-server subnet** A.B.C.D/M SWITCH(config)#**no ip dhcp-server subnet** A.B.C.D/M
Description	Configure subnet information and enter subnet configuration mode. At least one correct subnet configuration is required for the server to start properly.

- Configuring Subnet Address Ranges

Command	SWITCH(config-dhcp-subnet)# **range** A.B.C.D A.B.C.D SWITCH(config-dhcp-subnet)#**no range** A.B.C.D
Description	Configure the address range of the subnet. The server needs at least one assignable address range to start normally, which can be configured in the address pool below.

	It can be configured multiple times to configure different scopes.

- Configure subnet parameters

Command	SWITCH(config-dhcp-subnet)# **parameter** NAME VALUE SWITCH(config-dhcp-subnet)# **parameter (authoritative (on|off) | server-name** NAME **| server-identifier** IDENTIFY **| default-lease-time** <1-2147483648> **| max-lease-time** <1-2147483648> **| ping-timeout-ms** <1-65535> **| ping-timeout** <1-65535>**)** SWITCH(config-dhcp-subnet)#**no parameter** NAME SWITCH(config-dhcp-subnet)#**no parameter (authoritative | server-name | server-identifier | default-lease-time | max-lease-time | ping-timeout-ms | ping-timeout)**
Description	Configuration parameter information. Optional.

- Configure subnet options

Command	SWITCH(config-dhcp-subnet)# **option** NAME VALUE SWITCH(config-dhcp-subnet)# **option (routers** A.B.C.D **| domain-name** NAME **| domain-name-servers** A.B.C.D **| capwap-ac-v4** A.B.C.D**)** SWITCH(config-dhcp-subnet)#**no option** NAME SWITCH(config-dhcp-subnet)#**no option (routers | domain-name | domain-name-servers | capwap-ac-v4)**
Description	Configure option information. Usually, you need to configure the gateway routing address and DNS server address of the subnet. Optional.

31.2.2. Address Pool Configuration Commands

- Configuring address pool information

Command	SWITCH(config-dhcp-subnet)# **pool** NAME

	SWITCH(config-dhcp-subnet)#**no pool** NAME
Description	Configure the address pool in subnet mode. Subnets can be further divided through address pools and used on demand. Optional.

- Configure the address range of the address pool

Command	SWITCH(config-dhcp-pool)# **range** A.B.C.D A.B.C.D SWITCH(config-dhcp-pool)#**no range** A.B.C.D
Description	Configure the address range of the address pool. The server needs at least one assignable address range to start normally, which can be configured in the above subnet. It can be configured multiple times to configure different scopes.

- Configure address pool parameters

Command	SWITCH(config-dhcp-pool)# **parameter** NAME VALUE SWITCH(config-dhcp-pool)# **parameter (authoritative (on|off) | server-name** NAME **| server-identifier** IDENTIFY **| default-lease-time** <1-2147483648> **| max-lease-time** <1-2147483648> **| ping-timeout-ms** <1-65535> **| ping-timeout** <1-65535>**)** SWITCH(config-dhcp-pool)#**no parameter** NAME SWITCH(config-dhcp-pool)#**no parameter (authoritative | server-name | server-identifier | default-lease-time | max-lease-time | ping-timeout-ms | ping-timeout)**
Descrip[tion	Configuration parameter information. Optional.

- Configure address pool options

Command	SWITCH(config-dhcp-pool)# **option** NAME VALUE

	SWITCH(config-dhcp-pool)# **option (routers** A.B.C.D **| domain-name** NAME **| domain-name-servers** A.B.C.D **| capwap-ac-v4** A.B.C.D**)** SWITCH(config-dhcp-pool)#**no option** NAME SWITCH(config-dhcp-pool)#**no option (routers | domain-name | domain-name-servers | capwap-ac-v4)**
Description	Configure option information. Usually, you need to configure the gateway routing address and DNS server address of the address pool. Optional.

- Configure conditional filtering instructions

Command	SWITCH(config-dhcp-pool)# **(allow|deny|ignore)** CLASSNAME SWITCH(config-dhcp-pool)# **(allow|deny|ignore) (known-clients|unknown-clients|bootp|duplicates|declines)** SWITCH(config-dhcp-pool)# **no (allow|deny|ignore) (**CLASSNAME**|known-clients|unknown-clients|bootp|duplicates|declines)**
Description	Configure address pool filter conditions. For custom CLASSNAME, refer to Configuring Custom Classes in Global Configuration. Optional.

31.3. CONFIGURE CASE

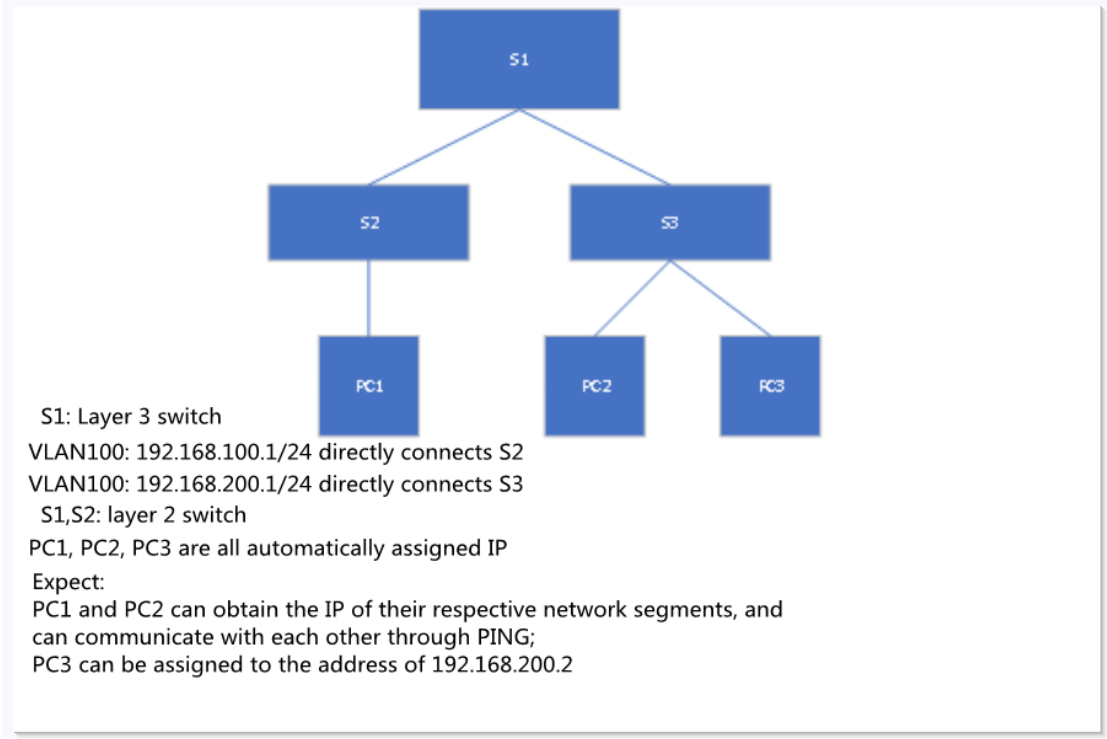
31.3.1. Conventional DHCP Server Address Assignment Scenario

4) Requirements

- See the description of the network diagram

5) Networking figure

Figure 1-1 Typical networking diagram of a DHCP server



Note: The MAC address of PC3 during the test is 00:0E:C6:C1:38:41

6) Typical configuration case

S1:

```
SWITCH(config)# ip dhcp-server subnet 192.168.100.0/24
SWITCH(config-dhcp-subnet)#range 192.168.100.2 192.168.100.254
SWITCH(config-dhcp-subnet)#option routers 192.168.100.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)# ip dhcp-server subnet 192.168.200.0/24
SWITCH(config-dhcp-subnet)#range 192.168.200.2 192.168.200.254
SWITCH(config-dhcp-subnet)#option routers 192.168.200.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)# ip dhcp-server static-lease pc3 00:0E:C6:C1:38:41
192.168.200.2
SWITCH(config)#ip dhcp-server option domain-name-servers 114.114.114.114
SWITCH(config)#ip dhcp-server enable
```

S2/S3: Empty configuration transparent transmission

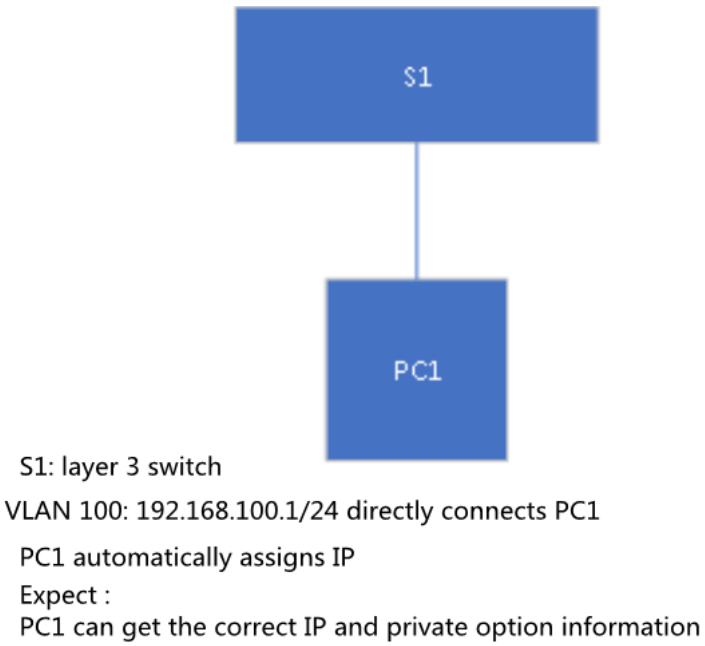
31.3.1. DHCP server address allocation scenarios that support private attribute delivery

1) requirements

- See the description of the network figure

2) Network figure

Figure 1-2 Typical networking diagram of a DHCP server



3) Typical configuration case

S1:

```
SWITCH(config)# ip dhcp-server custom-space dkwl code width 1 length
width 1
SWITCH(config)# ip dhcp-server custom-option dkwl.name code 1 string
SWITCH(config)# ip dhcp-server custom-option dkwl.ip code 2 ip-address
SWITCH(config)# ip dhcp-server custom-option vendor_dkwl code 43
encapsulate dkwl
SWITCH(config)# ip dhcp-server option dkwl.ip 1.1.1.1
SWITCH(config)# ip dhcp-server option dkwl.name "dockeer"
SWITCH(config)# ip dhcp-server subnet 192.168.100.0/24
SWITCH(config-dhcp-subnet)#range 192.168.100.2 192.168.100.254
SWITCH(config-dhcp-subnet)#option routers 192.168.100.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)#ip dhcp-server option domain-name-servers 114.114.114.114
SWITCH(config)#ip dhcp-server enable
```

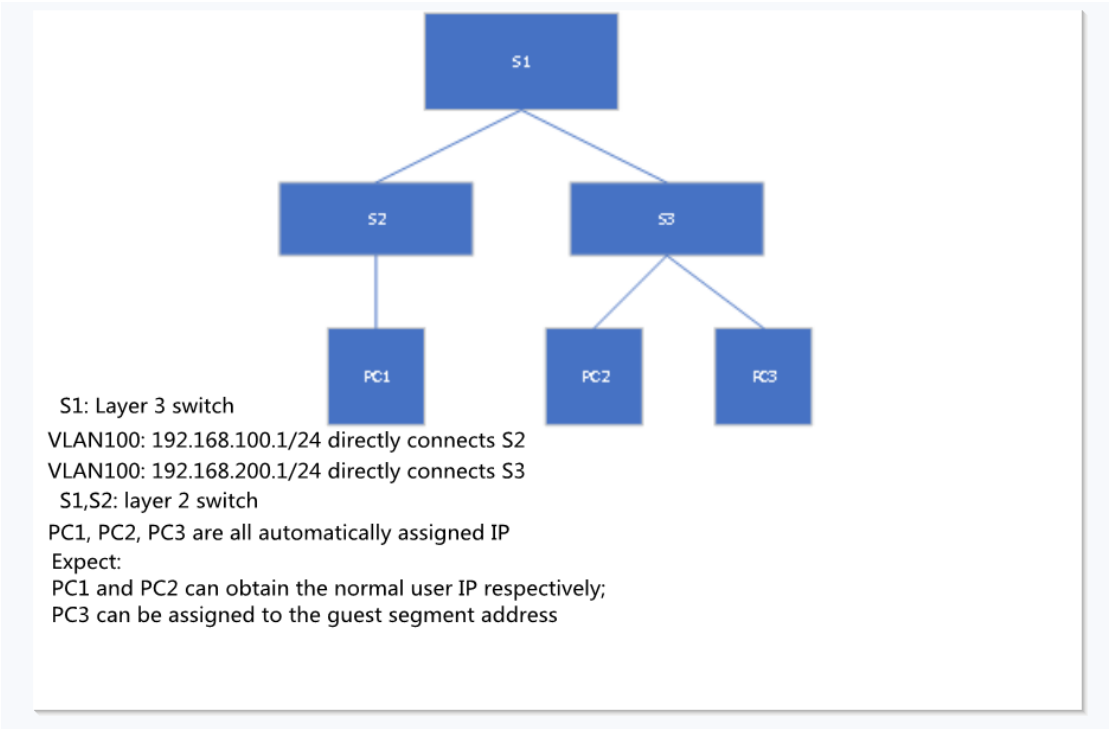
31.3.1. DHCP Server Address Assignment Scenario Supporting Guest Separation

1) Requirements

- See the description of the network figure
- Normal user assigned address 192.168.100.2-192.168.100.100 and 192.168.200.2-192.168.200.100
- Guest Assigned Address192.168.100.200-192.168.100.254

2) Networking figure

Figure 1-3 Typical networking diagram of a DHCP server



3) Typical configuration case

S1:

```
SWITCH(config)# ip dhcp-server subnet 192.168.100.0/24
SWITCH(config-dhcp-subnet)#range 192.168.100.2 192.168.100.100
SWITCH(config-dhcp-subnet)#option routers 192.168.100.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)# ip dhcp-server subnet 192.168.200.0/24
SWITCH(config-dhcp-subnet)#pool employee
SWITCH(config-dhcp-pool)#range 192.168.200.2 192.168.200.100
SWITCH(config-dhcp-pool)#deny unknown-clients
SWITCH(config-dhcp-pool)#pool guest
SWITCH(config-dhcp-pool)#range 192.168.200.200 192.168.200.254
SWITCH(config-dhcp-pool)#allow unknown-clients
```

```
SWITCH(config-dhcp-pool)#exit
SWITCH(config-dhcp-subnet)#option routers 192.168.200.1
SWITCH(config-dhcp-subnet)#exit
SWITCH(config)#ip dhcp-server option domain-name-servers 114.114.114.114
SWITCH(config)#ip dhcp-server enable
```

S2/S3：Empty configuration transparent transmission

31.4. DISPLAY COMMAND

- Dispaly DHCP server state information

```
SWITCH#show ip dhcp-server status
DHCP Server: Enable (conf.Enable)
```

- Display address assignment information

```
SWITCH#show ip dhcp-server leases

Name              MAC               IP              Begin               End                 Manufacturer
----------------- ----------------- --------------- ------------------- ------------------- ----------------

liulang-work      00:0e:c6:c1:38:4a 3.3.3.254       1970-01-01 00:00:36 1970-01-01 00:10:36 ASIX ELECTRONICS CORP.
```

32. TROUBLESHOOTING

32.1. PING/TRACEROUT

- Execute the ping function

Command	SWITCH#**ping {ip** IPADDR **| ipv6** IPV6ADDR**}**
Description	Execute ping command

- Excute traceroute function

Command	SWITCH# **traceroute {ip** IPADDR **| ipv6** IPV6ADDR **}**
Description	Execute traceroute command

32.2. OPTICAL MODULE INFORMATION DETECTION

- Display port optical/copper module information

This command is used to display the information of the optical/copper module inserted on the optical port.

Command	SWITCH#**show interface {**IFNAME **|} optical-transceiver {info |}**
Description	If no interface-id is specified, the module information of all ports will be displayed If info is not specified, the DDM information of the port module will be displayed, and if z is specified, the complete module information (basic information, alarm information, manufacturer information) will be displayed.

Display all port module DDM information

DDM information display elements are as follows:

Fields	Illustration
Temp	The current operating temperature of the module, in °C, accurate to 1°C.
Voltage	The current working voltage of the module, in V, accurate to 0.01V.
Bias	The current working current of the module, in mA, accurate to 0.01mA.
RX power	The current received optical power of the module, in dBm, accurate to 0.01dBM.
TX power	The current transmit optical power of the module, in dBm, accurate to 0.01dBM.
OK	normal, no intervention required
WARN	Alarm, indicating that the device exceeds the allowable range and needs attention.

ALARM	Abnormal, indicating that the device's allowable state is seriously exceeded and immediate intervention is required.
ABSENT	absent
NA	Port not supported/module not supported
TIMEOUT	time out
ERR	mistake

```
SWITCH#show interface optical-transceiver
  Port      Temp        Voltage       Bias          RX power       TX power
            [C]           [V]         [mA]           [dBm]          [dBm]
-------- ---------- ------------- ------------- ------------- ------------
-
GiEO/9    42(OK)       3.20(OK)      32.34(OK)     -3.98(OK)      1.64(OK)
GiEO/10   ABSENT         ABSENT          ABSENT        ABSENT         ABSENT
GiEO/11   ABSENT         ABSENT          ABSENT        ABSENT         ABSENT
GiEO/12   ABSENT         ABSENT          ABSENT        ABSENT         ABSENT
```

- **Display port optical module/copper module general information:**

The overall information display elements of the module are as follows:

Operation error message

Fields	Illustration
Transceiver absent!	Failed to get information, maybe the module is not in place
Get transceiver info timeout!	Timeout to get information, need to get it again
Port doesn't support get module info!	The port does not support getting module information

Basic information

Fields	Illustration
Transceiver Type	Transceiver Type
Connector Type	Connector Type
Wavelength(nm)	Wavelength(nm)
Link Length	Supported link lengths
Digital Diagnostic Monitoring	Whether to support DDM function
Vendor Serial Number	Module serial number

Alarm information

Fields	Illustration
RX Channel loss of signal	RX Channel loss of signal
RX Channel power high	High received optical power alarm
RX Channel power low	Low received optical power alarm
TX Channel fault	Send Error
TX Channel bias high	Bias current high alarm
TX Channel bias low	Bias current low alarm
TX Channel power high	Sending high optical power alarm

TX Channel power low	Sending low optical power alarm
Temperature high	High temperature alarm
Temperature low	Low temperature alarm
Voltage high	High voltage alarm
Voltage low	Low voltage alarm
None	No alarm
This module doesn't support getting alarm!	The module does not support getting alarm information

Vendor information

Fields	Illustration
Vendor Name	Vendor Name
Vendor OUI	Vendor OUI
Vendor Part Number	Vendor Part Number
Vendor Revision	Vendor Revision number
Manufacturing Date	Manufacturing Date
Encoding	encoding type

```
SWITCH#show interface gigabitEthernet0/9 optical-transceiver info
#####################################################
                  gigabitEthernet0/9
+-------------------------------------------------+
|Transceiver base information:                    |
+-------------------------------------------------+
|Transceiver Type    :  1000BASE-ZX-SFP           |
|Connector Type      :  LC                        |
|Wavelength(nm)      :  1550                      |
|Link Length     :                                |
|    SMF fiber                                    |
|        -- 80km                                  |
|Digital Diagnostic Monitoring  : YES             |
|Vendor Serial Number           : WT1703230031    |
+-------------------------------------------------+
|Transceiver current alarm information:           |
+-------------------------------------------------+
|None                                             |
+-------------------------------------------------+
|Transceiver vendor information:                  |
+-------------------------------------------------+
|Vendor Name         : OEM                        |
|Vendor OUI          : 000000                     |
|Vendor Part Number  : SFP-GE-ZX-SM1550           |
|Vendor Revision     : V2                         |
```

```
|Manufacturing Date  : 2017-03-25                |
|Encoding            : 8B10B                     |
+------------------------------------------------+
```

32.3. DYING-GASP

The Dying-gasp function is for the moment when the power supply of the device is cut off, relying on the energy storage device such as the internal capacitor of the device to supply power for 10-20ms, and supports the device to issue a power failure alarm message.

According to the definition in 802.3ah, when a device power-down event occurs, the device sends an OAM event packet to its connected device. Since OAM is a point-to-point protocol, after the power-down event packet is sent to the next OAM-enabled device, Continue forwarding. A device that receives a power-down event will output a power-down LOG prompt.

In addition to the OAM alarm information, the power-down device will also send a trap message to the smmp server.

Node information	Data
Mib files	DOT3-OAM-MIB.mib
oid	1, 3, 6, 1, 2, 1, 158, 1, 6, 1, 4
value	dyingGaspEvent(257)

- Enable dying-gasp function

Command	SWITCH(config)#**dying-gasp enable** SWITCH(config)#**no dying-gasp**
Description	Turn on/off the dying-gasp function

LOG information

Dying gasp alarm log：”Device 00:d0:f8:c8:23:12 power down.”